Chapter 4

The Arithmetic of $\mathbb{Z}$

In this chapter, we start by introducing the concept of congruences; these are used in our proof (going back to Gauss[1]) that every integer has a unique prime factorization. Finally, we discuss the Euclidean Algorithm; we shall see later that the same method also works polynomial rings $K[X]$ over fields K.

4.1 Divisibility

Just as subtraction was not defined for all pairs of natural numbers (in $\mathbb{N}$, we could have defined $m - n$ for $m, n \in \mathbb{N}$ with $m \geq n$), division is not defined for all pairs of nonzero integers. The theory of divisibility studies this observation in more detail. We say that an integer $b \in \mathbb{Z}$ divides $a \in \mathbb{Z}$ (and write $b \mid a$) if there exists an integer $q \in \mathbb{Z}$ such that $a = bq$.

The main properties of the divisibility relation follow directly from the definition:

Proposition 4.1. *For any integers $a, b, c \in \mathbb{Z}$, we have*

1. $1 \mid a$, $a \mid a$, *and* $a \mid 0$;
2. *if* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$;
3. *if* $a \mid b$ *and* $a \mid c$, *then* $a \mid (b \pm c)$;
4. *if* $a \mid b$, *then* $(-a) \mid b$, $a \mid (-b)$, *and* $(-a) \mid (-b)$;
5. *if* $a \mid b$ *and* $b \neq 0$ *then* $|a| \leq |b|$;
6. *if* $a \mid b$ *and* $b \mid a$, *then* $|a| = |b|$.

Proof. These are formal consequences of the definition:

1. $a = a \cdot 1$; $0 = 0 \cdot a$.

[1] Carl-Friedrich Gauss: 1777 (Braunschweig, Germany) – 1855 (Göttingen, Germany)

2. We have $b = aq$ and $c = br$ for some integers $q, r \in \mathbb{Z}$; but then $c = br = a(qr)$, hence $a \mid c$.

3. We have $b = aq$ and $c = ar$ for integers q, r; then $b \pm c = a(q \pm r)$ implies that $a \mid (b \pm c)$.

4. If $b = aq$, then $b = aq = (-a)(-q)$ and $-b = a \cdot (-q) = (-a)q$.

5. We have $b = aq$ for some $q \in \mathbb{Z}$; since $b \neq 0$, we deduce that $q \neq 0$, hence $|q| \geq 1$ and therefore $|b| = |aq| \geq |a|$.

6. The claim is trivial if $a = b = 0$. If $a \neq 0$, then $b \mid a$ implies $b \neq 0$, and similarly $b \neq 0$ implies $a \neq 0$. By the preceding result we therefore have $|a| \leq |b|$ and $|b| \leq |a|$, hence $|a| = |b|$.

□

Elements dividing 1 are called units; the units in $\mathbb{Z}$ are -1 and $+1$. First of all, they are units because they divide 1. Now assume that $r \in \mathbb{Z}$ is a unit; then there exists an element $s \in \mathbb{Z}$ with $rs = 1$. Clearly $r, s \neq 0$, hence $|r|, |s| \geq 1$. If $|r| > 1$, then $0 < |s| < 1$, but there are no integers strictly between 0 and 1.

4.2 Congruences

Congruences are a very clever notation invented by Gauss (and published in 1801 in his "Disquisitiones Arithmeticae") to denote the residue of a number a upon division by a nonzero integer m. More precisely, he wrote $a \equiv b \bmod m$ if $m \mid (a - b)$. for elements $a, b, m \in \mathbb{Z}$.

The rules for divisibility can now be transferred painlessly to congruences: first we observe

Proposition 4.2. *Congruence between integers is an equivalence relation.*

Proof. Recall that a relation is called an equivalence relation if it is reflexive, symmetric and transitive. In our case, we have to show that the relation $\equiv$ has the following properties:

- reflexivity: $a \equiv a \bmod m$;
- symmetry: $a \equiv b \bmod m$ implies $b \equiv a \bmod m$;
- transitivity: $a \equiv b \bmod m$ and $b \equiv c \bmod m$ imply $a \equiv c \bmod m$

for $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{Z} \setminus \{0\}$.

The proofs are straightforward. In fact, $a \equiv a \bmod m$ means $m \mid (a-a)$, and every integer $m \neq 0$ divides 0. Similarly, $a \equiv b \bmod m$ is equivalent to $m \mid (a-b)$; but this implies $m \mid (b - a)$, hence $b \equiv a \bmod m$. Finally, if $a \equiv b \bmod m$ and $b \equiv c \bmod m$, then $m \mid (b - a)$ and $m \mid (c - b)$, hence m divides the sum $c - a = (c - b) + (b - a)$, and we find $a \equiv c \bmod m$ as claimed. □

Since $\equiv$ defines an equivalence relation, it makes sense to talk about equivalence classes. The equivalence class $[a]$ (or $[a]_m$ if we want to express the dependence on the modulus m) of an integer a consists of all integers $b \in \mathbb{Z}$ such that $b \equiv a \bmod m$; in particular, every residue class contains infinitely many integers. In the special case $m = 3$, for example, we have

$$\begin{aligned}
[0] &= \{\ldots, -6, -3, 0, 3, 6, \ldots\}, \\
[1] &= \{\ldots, -5, -2, 1, 4, 7, \ldots\}, \\
[2] &= \{\ldots, -4, -1, 2, 5, 8, \ldots\}, \\
[3] &= \{\ldots, -3, 0, 3, 6, 9, \ldots\} = [0],
\end{aligned}$$

etc. Note that $[0] = [3] = [6] = \ldots$ (in fact, $[0] = [a]$ for any $a \in [0]$), and similarly $[1] = [4] = \ldots$. In general, we have $[a] = [a']$ if and only if $a \equiv a' \bmod m$, that is, if and only if $m \mid (a - a')$.

In the case $m = 3$, there were exactly 3 different residue classes modulo 3, namely $[0]$, $[1]$, and $[2]$ (or, say, $[0]$, $[1]$, and $[-1]$ since $[-1] = [2]$). This holds in general:

Lemma 4.3. *For any integer $m > 1$, there are exactly m different residue classes modulo m, namely*

Proof. We first show that these classes are pairwise distinct. To this end, assume that $[a] = [b]$ for $0 \le a, b < m$; this implies $b \in [a]$, hence $a \equiv b \bmod m$ or $m \mid (b - a)$: but since $|b - a| < m$, this can only happen if $a = b$.

Next, there are no other residue classes: given any class $[a]$, we write $a = mq + r$ with $0 \le r < m$ (the division algorithm at work again), and then $[a] = [r]$ is one of the classes listed above. $\square$

The set $\{0, 1, 2, \ldots, m - 1\}$ is often called a complete set of representatives modulo m for this reason. Sometimes we write $r + m\mathbb{Z}$ instead of $[r]$.

The one thing that makes congruences *really* useful is the fact that we can define a ring structure on the set of residue classes. This is fundamental, so let us do this in detail.

The elements of our ring $\mathbb{Z}/m\mathbb{Z}$ will be the residue classes $[0]$, $[1]$, ..., $[m-1]$ modulo m. We have to define an addition and a multiplication and then verify the ring axioms.

• Addition $\oplus$: Given two classes $[a]$ and $[b]$, we put $[a] \oplus [b] = [a + b]$. We have to check that this is well defined: assume that $[a] = [a']$ and $[b] = [b']$; then we have to show that $[a + b] = [a' + b']$. But this is easy: we have $a - a' \in m\mathbb{Z}$, say $a - a' = mA$, and similarly $b - b' = mB$. But then $(a + b) - (a' + b') = m(A + B) \in m\mathbb{Z}$, hence $[a + b] = [a' + b']$.

The neutral element is the residue class $[0] = m\mathbb{Z}$, and the inverse element of $[a]$ is $[-a]$, or, if you prefer, $[m - a]$. In fact, we have $[a] \oplus [0] = [a + 0] = [a]$ and $[a] \oplus [-a] = [a + (-a)] = [0]$. The law of associativity and the commutativity are inherited from the corresponding properties of integers: since e.g. $(a + b) + c = a + (b + c)$, we have $([a] \oplus [b]) \oplus [c] = [a] \oplus ([b] \oplus [c])$.

• Multiplication $\odot$: of course we put $[a] \odot [b] = [ab]$. The verification that this is well defined is left as an exercise. The neutral element is the class $[1]$.

• Distributive Law: Again, $([a] \oplus [b]) \odot [c] = [a] \odot [c] \oplus [b] \odot [c]$ follows from the corresponding properties of integers.

Theorem 4.4. *The residue classes* $[0]$, $[1]$, $\ldots$, $[m-1]$ *modulo* m *form a ring* $\mathbb{Z}/m\mathbb{Z}$ *with respect to addition* $\oplus$ *and multiplication* $\odot$.

Now that we have introduced the rings that we will study for some time to come, we simplify the notation by writing $+$ and $\cdot$ instead of $\oplus$ and $\odot$. Moreover, we will drop our references to classes and deal only with the integers representing them; in order to make clear that we are dealing with residue classes, we write $\equiv$ instead of $=$ and add a "mod m" at the end. What this means in practice is that we identify $\mathbb{Z}/m\mathbb{Z}$ with the set of integers $\{0, 1, \ldots, m-1\}$.

4.3 Unique Factorization in $\mathbb{Z}$

An integer $n \neq 0, \pm 1$ is called irreducible if it only admits trivial factors, that is, if $n = ab$ for $a, b \in \mathbb{Z}$ implies $a = \pm 1$ or $b = \pm 1$. In elementary number theory, irreducible elements are often called primes; we shall reserve that name for integers $p \neq 0, \pm 1$ with the property that $p \mid ab$ for $a, b \in \mathbb{Z}$ implies $p \mid a$ or $p \mid b$.

For example, 2 is prime because $2 \mid ab$ implies that $2 \mid a$ or $2 \mid b$ (proof by contradiction).

The first step in proving unique factorization is showing that primes and irreducibles are the same. One direction is immediate:

Proposition 4.5. *Primes are irreducible.*

Proof. Assume not. Then $p = rs$ with $r, s \in \mathbb{Z}$ nonunits. In particular, $p \mid rs$. If we can show that $p \nmid r$ and $p \nmid s$, then p cannot be prime and we have won.

So assume that $p \mid r$, i.e. $r = pt$ for some $t \in \mathbb{Z}$; since we also have $p = rs$, we find $p = rs = pst$, hence $st = 1$, and this shows that s and t are units. This contradicts the assumption that s is a nonunit: thus $p \nmid r$. Similarly, $p \nmid s$. $\square$

Before we can prove that irreducibles are prime, we need

Proposition 4.6. *If* p *is irreducible, then* $\mathbb{Z}/p\mathbb{Z}$ *is a field.*

Proof. We have to show that if $[a] \neq [0]$, i.e., if $0 < a < p$, then there exists a residue class $[b]$ such that $[ab] = [1]$.

This is trivial if $a = 1$, so assume $a > 1$ and put $r_1 = \lceil p/a \rceil$; then $0 \leq ar_1 - p < a$. If we had $ar_1 - p = 0$, then the fact that p is irreducible implies $a = 1$ or $a = p$, contradicting our assumption. Thus $0 < ar_1 - p < a$.

If $a_1 = ar_1 - p = 1$, then $b = r_1$ is the inverse of a; if $a_1 > 1$, then put $r_2 = \lceil p/a_1 \rceil$ and repeat the above argument. If $a_1 r_2 - p = 1$, then $[ar_1 r_2] = [1]$, and $b = r_1 r_2$ is the desired inverse of a. Since a_i decreases by at least 1 in each step, the process must eventually terminate. $\square$

Fields F have very nice properties; one of them is that linear equations $ax = b$ with $a, b \in F$ and $a \neq 0$ always have a unique solution: in fact, since $a \neq 0$, it has an inverse element $a^{-1} \in F$, and multiplying through by a^{-1} we get $x = a^{-1}b$. This does not work in general rings: the equation $2x = 1$ does not have a solution in $\mathbb{Z}/4\mathbb{Z}$, and the linear equation $2x = 2$ has two solutions, namely $x = [1]$ and $x = [3]$.

The main result on which unique factorization will be built is the following:

Proposition 4.7. *Irreducibles in $\mathbb{Z}$ are prime.*

Proof. Assume that p is irreducible and that $p \mid ab$. If $p \nmid a$ and $p \nmid b$, then $[a]$ and $[b]$ are invertible modulo p; but then $[ab]$ has an inverse (if $[a][r] = [b][s] = [1]$, then $[ab][rs] = [1]$), and therefore $p \nmid ab$. This proves that $p \mid a$ or $p \mid b$. $\square$

Our first result in the direction of the Unique Factorization Theorem is quite innocent:

Proposition 4.8. *Every integer $n > 1$ has a prime factorization.*

Proof. We proceed by induction. We call an integer n "nice" if it has a prime factorization. Clearly $n = 2$ is nice because 2 is prime. Now assume that all integers $< n$ are nice; since $n > 1$, it is either prime (and thus nice) or it isn't; but if n is not prime, then n is not irreducible (since primes and irreducibles are the same), so n has proper divisors, say $n = ab$ with $a, b \in \mathbb{N}$. Since $a, b < n$, these factors are nice, hence they have prime factorizations, say $a = p_1 \cdots p_r$ and $b = q_1 \cdots q_s$. But then $n = p_1 \cdots p_r q_1 \cdots q_s$ is a prime factorization of n. $\square$

We also can attach a prime factorization to negative integers: if $n < 0$ and $-n = p_1 \cdots p_r$ is a prime factorization of $-n > 0$, then $n = -p_1 \cdots p_r$ is a prime factorization of n.

Note that we have talked about "a" prime factorization; as a matter of fact, the prime factorization of an integer n is essentially unique, but this needs to be proved.

Again you may think that this is obvious; after all, if, say, 11 divides an integer n, then there cannot be a prime factorization of n that does not contain 11 as a factor. Or can there?

Consider the set $S = \{1, 5, 9, 13, \ldots\}$ of positive integers of the form $4n + 1$. Let us call a number $p > 1$ in S irreducible if its only divisors in S are 1 and p. Thus 5 and 9 are irreducible, while 25 is not. Here every integer has a factorization into irreducibles, but it is not unique: for example, $21 \cdot 33 = 9 \cdot 77$, and 9, 21, 33 and 77 are all irreducible in S according to our definition. The reason why unique factorization fails is the existence of irreducibles that aren't prime: clearly $9 \mid 21 \cdot 33$ since $21 \cdot 33 = 9 \cdot 77$, but 9 does not divide 21 or 33.

While the set S considered above is multiplicatively closed (if $s, s' \in S$, then $ss' \in S$), it is not a ring. The next example is closer to being a ring: the set $2\mathbb{Z}$ of even integers would be a ring if it had a unit element (a ring without identity is sometimes called a rng). The rng $2\mathbb{Z}$ does not have unique factorization into irreducibles: We have $60 = 2 \cdot 30 = 6 \cdot 10$, and each of these factors is irreducible (reducible elements in $2\mathbb{Z}$ are necessarily divisible by 4).

The theorem of unique factorization asserts that every integer has a prime factorization, and that it is unique up to the order of the factors.

Theorem 4.9. *Every integer $n \geq 2$ has a prime factorization $n = p_1 \cdots p_r$ (with possibly repeated factors). This factorization is essentially unique, that is: if $n = p_1 \cdots p_r$ and $n = q_1 \cdots q_s$ are prime factorizations of an integer n, then $r = s$, and we can reorder the q_j in such a way that $p_j = q_j$ for $1 \leq j \leq r$.*

A partial result in the direction of Theorem 4.9 can already be found in Euclid's elements; the first explicit statement and proof was given by Gauss in 1801.

Proof. We already know that prime factorizations exist, so we only have to deal with uniqueness. This will be proved by induction on $\min\{r, s\}$, i.e. on the minimal number of prime factors of n. We may assume without loss of generality that $r \leq s$.

If $r = 0$, then $n = 1$, and $n = 1 = q_1 \cdots q_s$ implies $s = 0$.

Now assume that every integer that is a product of at most $r - 1$ prime factors has a unique prime factorization, and consider $n = p_1 \cdots p_r = q_1 \cdots q_s$. Since p_1 is a prime that divides $n = q_1 \cdots q_s$, it must divide one of the factors, say $p_1 \mid q_1$ (after rearranging the q_i if necessary). But q_1 is prime, so its only positive divisors are 1 and q_1; since p_1 is a prime, it is a nonunit, and we conclude that $p_1 = q_1$. Canceling p_1 shows that $p_2 \cdots p_r = q_2 \cdots q_s$, and by induction assumption we have $r = s$, and $p_j = q_j$ after rearranging the q_i if necessary. □

Remark. There is a simple reason for doing induction on the minimal number of prime factors and not simply on the number of prime factors of n: the fact that the number of prime factors of an integer is well defined is a consequence of the result we wanted to prove!

Some Applications

The Infinitude of Primes

How many primes are there? Euclid gave an ingenious proof that there are infinitely many:

Proposition 4.10. *There are infinitely many primes.*

Proof. We give a proof by contradiction. Assume that there are only finitely many primes, namly $p_1 = 2, \ldots, p_r$, and consider the integer $N = p_1 \cdots p_r + 1$. Then $N > 1$, hence it is divisible by a prime p. This prime p is not in our list: if we had $p = p_i$, then $p \mid N$ and $p \mid N - 1 = p_1 \cdots p_i \cdots p_r$, hence p divides $1 = N - (N - 1)$: contradiction, because p is a prime, hence can't be a unit by definition. □

Narkiewicz's book 'The Development of the Prime Number Theorem' contains several proofs for the infinitude of Primes.

Proof 2. (Hermite[2]) For $n = 1, 2, \ldots$, let q_n denote the smallest prime divisor of $n! + 1$. Then $q_n > n$, hence there are infinitely many primes.

Proof 3 (Stieltjes[3] 1890): Assume that there are only finitely many primes, and let D denote their product. Let $D = mn$ be any factorization of D with $m, n \in \mathbb{N}$. Then for any prime p, we have $p \mid m$ or $p \mid n$, but not both; thus p does not divide $m + n$, so $m + n$ can't have any prime divisor: contradiction.

What I don't like here is that if you take the factorization $D = D \cdot 1$, then you get back Euclid's proof. Why on earth would anyone want to complicate a simple proof? □

We have already seen that integers are squares of rational numbers if and only if they are squares of integers. Here we shall use unique factorization to show that $\sqrt{p}$ is irrational. For assume not: then $p = r^2/s^2$ for $r, s \in \mathbb{N}$, and assume that r and s are coprime (if they are not, cancel). Thus $ps^2 = r^2$. Thus $p \mid r^2$, and since p is prime, we must have $p \mid r$, say $r = pt$. Then $ps^2 = p^2t^2$, hence $s^2 = pt^2$. But then $p \mid s^2$, hence $p \mid s$ since p is prime, and this is a contradiction, since we now have shown that $p \mid r$ and $p \mid s$ although we have assumed that they are coprime.

4.4 Greatest Common Divisors in $\mathbb{Z}$

We will now introduce greatest common divisors: we say that d is a greatest common divisor of $a, b \in \mathbb{Z}$ and write $d = \gcd(a, b)$ if d satisfies the following two properties:

1. $d \mid a$, $d \mid b$;
2. if $e \in \mathbb{Z}$ satisfies $e \mid a$ and $e \mid b$, then $e \mid d$.

We can use the unique factorization property to give a formula for the gcd of two integers. Before we do so, let us introduce some notation. We can write an $a \in \mathbb{Z}$ as a product of primes. In fact fact we can write $a = \pm \prod p_i^{a_i}$, where the product is over all irreducible elements p_1, p_2, p_3, $\ldots$, and where at most finitely many a_i are nonzero. In order to avoid the $\pm$ in our formulas, let us restrict to positive integers from now on.

Lemma 4.11. *For integers $a, b \in \mathbb{N}$ we have $b \mid a$ if and only if $b_i \leq a_i$ for all i, where $a = \prod p_i^{a_i}$ and $b = \prod p_i^{b_i}$ are the prime factorizations of a and b.*

Proof. We have $b \mid a$ if and only if there is a $c \in \mathbb{N}$ such that $a = bc$. Let $c = \prod p_i^{c_i}$ be its prime factorization. Then $c_i \geq 0$ for all i, and $a_i = b_i + c_i$, hence $b \mid a$ is equivalent to $a_i \geq b_i$ for all i. □

[2] Charles Hermite, 1822 (Dieuze, Lorraine, France) – 1901 (Paris).
[3] Thomas Jan Stieltjes, 1856 (Zwolle, The Netherlands) – 1894 (Toulouse, France)

Here's our formula for gcd's:

Theorem 4.12. *The gcd of two nonzero integers*

$$a = \prod p_1^{a_i} \quad and b = \prod p_i^{b_i}$$

is given by

$$d = \prod p_i^{\min\{a_i, b_i\}}.$$

Proof. We have to prove the two properties characterizing gcd's:

1. $d \mid a$ and $d \mid b$. But this follows immediately from Lemma 9.7.
2. If $d' \mid a$ and $d' \mid b$, then $d' \mid d$. In fact, write down the prime factorization $d' = \prod p_i^{d_i'}$ of d'. Then $d' \mid a$ and $d' \mid b$ imply $d_i' \le \min(a_i, b_i) = d_i$, hence $d' \mid d$.

Now assume that d and d' are gcd's of a and b. Then $d \mid d'$ by 2. since d' is a gcd, and $d' \mid d$ since d is a gcd, hence $d' = \pm d$. $\square$

For the ring $\mathbb{Z}$ of integers, we have much more than the mere existence of gcd's: the gcd of two integers $a, b \in \mathbb{Z}$ has a "Bezout representation",[4] that is, if $d = \gcd(a, b)$, then there exist integers $m, n \in \mathbb{Z}$ such that $d = am + bn$.

Theorem 4.13 (Bezout's Lemma). *Assume that $d = \gcd(a, b)$ for $a, b \in \mathbb{Z}$; then d has a Bezout representation.*

Proof. Consider the set $D = m\mathbb{Z} + n\mathbb{Z} = \{am + bn : a, b \in \mathbb{Z}\}$. Clearly D is a nonempty set, and if $c \in D$ then we also have $-c \in D$. In particular, D contains positive integers. Let d be the smallest positive integer in D; we claim that $d = \gcd(m, n)$. There are two things to show:
Claim 1: d is a common divisor of m and n. By symmetry, it is sufficient to show that $d \mid m$. Write $m = rd + s$ with $0 \le s < d$; we find $d = am + bn$, hence $s = rd - m = r(am + bn) - m = (ra - 1)m + bn \in D$. The minimality of d implies $s = 0$, hence $d \mid m$.
Claim 2: if e is a common divisor of m and n, then $e \mid d$. Assume that $e \mid m$ and $e \mid n$. Since $d = am + bn$, we conclude that $e \mid d$.

The existence of the Bezout representation is a simple consequence of the fact that $d \in D$. $\square$

Note that the key of the proof is the existence of a division with remainder.

Bezout's Lemma can be used to give an important generalization of the property $p \mid ab \Longrightarrow p \mid a$ or $p \mid b$ of primes p:

Proposition 4.14. *If $m \mid ab$ and $\gcd(m, b) = 1$, then $m \mid a$.*

Proof. Write $ab = mn$; by Bezout, there are $x, y \in \mathbb{Z}$ such that $mx + by = 1$. Multiplying through by a gives $a = max + aby = max + mny = m(ax + ny)$, that is, $m \mid a$. $\square$

[4] Etienne Bezout: 1730 (Nemours, France) – 1783 (Basses-Loges, France)

Finally, observe that canceling factors in congruences is dangerous: we have $2 \equiv 8 \bmod 6$, but not $1 \equiv 4 \bmod 6$. Here's what we're allowed to do:

Proposition 4.15. *If $ac \equiv bc \bmod m$, then $a \equiv b \bmod \frac{m}{\gcd(m,c)}$.*

Proof. We have $m \mid (ac-bc) = c(a-b)$. Write $d = \gcd(m,c)$, $m = dm'$, $c = dc'$, and note that $\gcd(m',c') = 1$. From $dm' \mid dc'(a-b)$ we deduce immediately that $m' \mid c'(a-b)$; since $\gcd(m',c') = 1$, we even have $m' \mid (a-b)$ by Prop 4.14, i.e. $a \equiv b \bmod \frac{m}{\gcd(m,c)}$. □

Proof 4 of the Infinitude of Primes. Let $F_n = 2^{2^n} + 1$ denote the nth Fermat number. We claim: If $m < n$, then $F_m \mid (F_n - 2)$. In fact, $F_n - 2 = 2^{2^n - 1}$ is divisible by $2^{2^{m+1}} - 1 = (2^{2^m} - 1)F_m$. Thus $\gcd(F_m, F_n) \mid (F_n, F_n - 2) = 2$, but Fermat numbers are odd, hence they are coprime.

4.5 The Euclidean Algorithm

In most modern textbooks, Unique Factorization is proved using the Euclidean algorithm; it has the advantage that a similar proof can also be used for other rings, e.g. polynomial rings $K[X]$ over fields K. The Euclidean algorithm is a procedure that computes the gcd of integers without using their prime factorization (which may be difficult to obtain if the numbers involved are large). Moreover, it allows us to compute a Bezout representation of this gcd (note that our proof of Thm. 4.13 was an existence proof, giving no hint at how to compute such a representation).

Given integers m and n, there are uniquely determined integers q_1 and r_1 such that $m = q_1 n + r_1$ and $0 \le r_1 < n$. Repeating this process with n and r_1, we get $n = r_1 q_2 + r_2$ with $0 \le r_2 < r_1$, etc. Since $n > r_1 > r_2 > \ldots \ge 0$, one of the r_i, say r_{n+1}, must eventually be 0:

$$\begin{aligned}
m &= q_1 n + r_1 && (4.1)\\
n &= q_2 r_1 + r_2 && (4.2)\\
r_1 &= q_3 r_2 + r_3 && (4.3)\\
&\ \ \ldots\\
r_{n-2} &= q_n r_{n-1} + r_n && (4.4)\\
r_{n-1} &= q_{n+1} r_n && (4.5)
\end{aligned}$$

Example: $m = 56$, $n = 35$

$$\begin{aligned}
56 &= 1 \cdot 35 + 21\\
35 &= 1 \cdot 21 + 14\\
21 &= 1 \cdot 14 + 7\\
14 &= 2 \cdot 7
\end{aligned}$$

Note that the last r_i that does not vanish (namely $r_3 = 7$) is the gcd of m and n. This is no accident: we claim that $r_n = \gcd(m,n)$ in general. For a proof, we have to verify two things:

Claim 1: r_n is a common divisor of m and n. Equation (4.5) shows $r_n \mid r_{n-1}$; plugging this into (4.4) we find $r_n \mid r_{n-2}$, and going back we eventually find $r_n \mid r_1$ from (4.3), $r_n \mid n$ from (4.2) and finally $r_n \mid m$ from (4.1). In particular, r_n is a common divisor of m and n.

Claim 2: if e is a common divisor of m and n, then $e \mid r_n$. This is proved by reversing the argument above: (4.1) shows that $e \mid r_1$, (4.2) then gives $e \mid r_2$, and finally we find $e \mid r_n$ from (4.5) as claimed.

The Euclidean algorithm does more than just compute the gcd: take our example $m = 56$ and $n = 35$; writing the third line as $\gcd(m,n) = 7 = 21 - 1\cdot 14$ and replacing the 14 by $14 = 35 - 1 \cdot 21$ coming from the second line we get $\gcd(m,n) = 21 - 1 \cdot (35 - 1 \cdot 21) = 2 \cdot 21 - 1 \cdot 35$. Now $21 = 56 - 1 \cdot 35$ gives $\gcd(m,n) = 2 \cdot (56 - 1 \cdot 35) - 1 \cdot 35 = 2 \cdot 56 - 3 \cdot 35$, and we have found a Bezout representation of the gcd of 56 and 35.

This works in complete generality: (4.4) says $r_n = r_{n-2} - q_n r_{n-1}$; the line before, which $r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$, allows us to express r_n as a $\mathbb{Z}$-linear combination of r_{n-2} and r_{n-3}, and going back we eventually find an expression of r_n as a $\mathbb{Z}$-linear combination of a and b.

Bezout representations have an important practical application: they allow us to compute multiplicative inverses in $\mathbb{Z}/p\mathbb{Z}$. In fact, let $[a]$ denote a nonzero residue class modulo p; since $\mathbb{Z}/p\mathbb{Z}$ is a field, $[a]$ must have a multiplicative inverse, that is, there must be a residue class $[b]$ such that $[ab] = [1]$. Since there are only finitely many residue classes, this can always be done by trial and error (unless p is large): for example, let us find the multiplicative inverse of $[2]$ in $\mathbb{Z}/5\mathbb{Z}$: multiplying $[2]$ successively by $[1]$, $[2]$, $[3]$, $[4]$ we find $[2] \cdot [3] = [6] = [1]$; thus $[2]^{-1} = [3]$ (we occasionally also write $\frac{1}{2} \equiv 3 \bmod 5$).

Computing the inverse of $[2]$ in $\mathbb{Z}/p\mathbb{Z}$ is actually always easy: note that we want an integer b such that $[2b] = [1]$; but $[1] = [p+1]$, hence we can always take $b = \frac{p+1}{2}$.

In general, however, computing inverses is done using Bezout representations. Assume that $\gcd(a,p) = 1$ (otherwise there is no multiplicative inverse), compute integers $x, y \in \mathbb{Z}$ such that $1 = ax + py$; reducing this equation modulo p gives $1 \equiv ax \bmod p$, i.e., $[a][x] = [1]$, or $[a]^{-1} = [x]$.

Exercises

4.1 Prove that $2 \mid n(n+1)$ for all $n \in \mathbb{N}$
  a) using induction
  b) directly.

4.2 Prove that $3 \mid n(n^2-1)$ for all $n \in \mathbb{N}$. Generalizations?

4.3 Prove that $8 \mid (n^2-1)$ for all odd $n \in \mathbb{N}$.

4.4 Prove or disprove: if $n \mid ab$ and $n \nmid a$, then $n \mid b$.

4.5 Show that there are arbitrary long sequences of composite numbers (Hint: observe that $2 \cdot 3 + 2$ and $2 \cdot 3 + 3$ can be seen to be composite without performing any division; generalize!)

4.6 Show that divisibility defines a *partial order* on $\mathbb{Z}$ by writing $a \le b$ if $b \mid a$.

4.7 Show that, for integers $a, b, c, d, m \in \mathbb{Z}$ with $m > 0$, we have

- $a \equiv b \bmod m \Longrightarrow a \equiv b \bmod n$ for every $n \mid m$;
- $a \equiv b \bmod m$ and $c \equiv d \bmod m \Longrightarrow a+c \equiv b+d \bmod m$ and $ac \equiv bd \bmod m$;
- $a \equiv b \bmod m \Longrightarrow ac \equiv bc \bmod m$ for any $c \in \mathbb{Z}$.

4.8 Show that there are infinitely many primes of the form $3n - 1$.

4.9 Try to extend the above proof to the case of primes of the form $3n + 1$ (and $5n - 1$). What goes wrong?

4.10 Show that primes $p = c^2 + 2d^2$ satisfy $p = 2$ or $p \equiv 1, 3 \bmod 8$.

4.11 Show that primes $p = c^2 - 2d^2$ satisfy $p = 2$ or $p \equiv 1, 7 \bmod 8$.

4.12 Show that primes $p = c^2 + 3d^2$ satisfy $p = 3$ or $p \equiv 1 \bmod 3$.

4.13 Compute $d = \gcd(77, 105)$ and write d as a $\mathbb{Z}$-linear combination of 77 and 105.

4.14 Check the addition and multiplication table for the ring $\mathbb{Z}/3\mathbb{Z}$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

4.15 Compute addition and multiplication tables for the rings $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$.

4.16 Compute the multiplicative inverse of [17] in $\mathbb{Z}/101\mathbb{Z}$.

4.17 Compute $\gcd(2^m - 1, 2^n - 1)$ for small values of $m, n \ge 1$ until you discover a general formula for d.

4.18 Let $U_1 = U_2 = 1$, and $U_{n+1} = U_n + U_{n-1}$ denote the Fibonacci numbers. Find a formula for $\gcd(U_m, U_n)$.

4.19 Show that the Fermat numbers $F_n = 2^{2^n} + 1$ are pairwise coprime.

4.20 Show that there are infinitely many primes of the form $p = 4n + 3$.

4.21 Show that there are infinitely many primes of the form $p = 3n + 2$.

4.22 Compute $\gcd(x^2+2x+2, x^2-x-2)$ over $\mathbb{Z}/m\mathbb{Z}$ for $m = 2, 3, 5$ and 7, and find its Bezout representation.

4.23 Let $a, b \in \mathbb{N}$ be coprime, and let $r \in \mathbb{N}$ be a divisor of ab. Put $u = \gcd(a, r)$ and $v = \gcd(b, r)$, and show that $r = uv$.

4.24 Assume that $M_p = 2^p - 1$ is a prime. List the complete set of (positive) divisors of $N_p = 2^{p-1}M_p$, and compute their sum. Conclude that if M_p is prime, then N_p is a perfect number (a number n is called perfect if the sum of its (positive) divisors equals $2n$).

Euler later proved that every even perfect number has the form $2^{p-1}M_p$ for some Mersenne prime M_p. It is conjectured (but not known) that odd perfect numbers do not exist.

4.25 Compute the last two digits of 27^{19}.

4.26 For primes $p \in \{3, 5, 7, 11, 13\}$, compute $A \equiv (\frac{p-1}{2})! \bmod p$. Can you find a pattern? If not, compute $B \equiv A^2 \bmod p$. Formulate a conjecture.

4.27 Check which of the primes $p \in \{3, 5, 7, 11, 13\}$ can be written as $p = a^2 + b^2$ with integers $a, b \in \mathbb{N}$ (e.g. $5 = 1^2 + 2^2$). Formulate a conjecture.

4.28 For some small primes $p = 4n + 1$, compute the smallest residue (in absolute value) of $a \bmod p$, where $a = \binom{2n}{n}$. (Example: for $p = 5$, we have $n = 1$ and $\binom{2}{1} = 2 \equiv 2 \bmod 5$.) Compare with the results from the preceding Exercise. Formulate a conjecture and test it for a few more primes.

4.29 a) Given a 5-liter jar and a 3-liter jar and an unlimited supply of water, how do you measure out 4 liters exactly?
b) Can you also measure out 1, 2 and 3 liters?
c) Which quantities can you measure out if you are given a 6-liter and a 9-liter jar?
d) Formulate a general conjecture. Can you prove it (at least partially)?

Chapter 5

Diophantine Equations

In this chapter, we will give a couple of applications of the number theory we have developed so far: the theorem of Girard[1]-Fermat[2] that primes of the form $4n+1$ are sums of two squares, the solution of the diophantine equation $x^2+y^2=z^2$, and Fermat's Last Theorem for the exponent 4.

5.1 Fermat's Two-Squares Theorem

A well known theorem first stated by Girard, and probably first proved by Fermat (the first known proof is due to Euler) concerns primes that are sums of two squares, such as $5=1^2+2^2$ or $29=2^2+5^2$. The following characterization of such primes is a simple consequence of the notion of congruences; the converse is also true, but much harder to prove.

Proposition 5.1. *If a prime p is the sum of two integral squares, then $p=2$ or $p \equiv 1 \bmod 4$.*

Proof. There are 4 residue classes modulo 4; their squares are $[0]=[0]^2$ and $[1]=[1]^2$, and in fact the squares $[2]^2=[0]$ and $[3]^2=[1]$ of the remaining classes don't produce new ones.

Now assume that $p=a^2+b^2$. Since $a^2, b^2 \equiv 0, 1 \bmod 4$, we find that a^2+b^2 must be congruent modulo 4 to one of $0=0+0$, $1=1+0=0+1$, or $2=1+1$, that is, $p \equiv 0, 1, 2 \bmod 4$. Since no prime is congruent to 0 mod 4, and since 2 is the only prime $\equiv 2 \bmod 4$, we even have $p=2$ or $p \equiv 1 \bmod 4$ as claimed. $\square$

For the converse, we need to know when $[-1]$ is a square in $\mathbb{Z}/p\mathbb{Z}$ for primes p. Experiments show that $[-1]$ is not a square modulo 3, 7, or 11, and that $[2]^2=[-1]$ for $p=5$, and $[5]^2=[-1]$ for $p=13$. The general result is

[1] Albert Girard (?), 1595 (St Mihiel, France) – 1632 (Leiden, Netherlands)

[2] Pièrre de Fermat, ca. 1607 (Beaumont-de-Lomagne, near Toulouse, France) –1665 (Castres, France)

Proposition 5.2. *Let p be an odd prime; then the congruence $a^2 \equiv -1 \bmod p$ has a solution if and only if $p \equiv 1 \bmod 4$.*

For the proof, we need some auxiliary results.

Proposition 5.3 (Wilson's Theorem). *For $p > 1$, we have $(p-1)! \equiv -1 \bmod p$ if and only if p is a prime.*

Proof. Let p be a prime; the claim is trivial if $p = 2$, so assume that p is odd. The idea is to look at pairs of the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$. In fact, for every $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ there is an element $a^{-1} \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $a \cdot a^{-1} \equiv 1 \bmod p$. In general, $[a]$ and $[a^{-1}]$ are different: $[a] = [a^{-1}]$ implies $[a^2] = [1]$, so this can only happen (and does in fact happen) if $[a] = [1]$ or $[a] = [-1] = [p-1]$ (here we use that $\mathbb{Z}/p\mathbb{Z}$ is a field; in fields, polynomials of degree 2 such as $x^2 - 1$ have at most 2 roots).

Thus $(\mathbb{Z}/p\mathbb{Z})^\times \setminus \{[-1], [+1]\}$ is the union of pairs $\{[a], [a^{-1}]\}$ with $[a] \neq [a^{-1}]$, hence the product over all elements of $(\mathbb{Z}/p\mathbb{Z})^\times \setminus \{[-1], [+1]\}$ must be $[1]$. We can get $[(p-1)!]$ by multiplying this product with the two missing classes $[1]$ and $[-1]$, and this gives the claimed result $[(p-1)!] = [-1]$.

We still have to prove the converse: assume that $(n-1)! \equiv -1 \bmod n$; if p is a prime divisor of n, this congruence implies $(n-1)! \equiv -1 \bmod p$. But $p < n$ also implies that p occurs as a factor of $(n-1)!$ on the left hand side, hence we would have $0 \equiv (n-1)! \bmod p$. But then $0 \equiv -1 \bmod p$, a contradiction. ☐

Note that Wilson's theorem provides us with a primality test; unfortunately the only known way to compute $(n-1)!$ is via $n-2$ multiplications, so it takes even longer than trial division!

Proposition 5.4. *Let p be an odd prime and put $a = (\frac{p-1}{2})!$; then we have $a^2 \equiv (-1)^{(p+1)/2} \bmod p$. In particular, $a \equiv \pm 1 \bmod p$ if $p \equiv 3 \bmod 4$, and $a^2 \equiv -1 \bmod p$ if $p \equiv 1 \bmod 4$.*

Proof. We start with Wilson's theorem $(p-1)! \equiv -1 \bmod p$; if, in the product $(p-1)!$, we replace the elements $\frac{p+1}{2}, \frac{p+3}{2}, \ldots, p-1$ by their negatives $-\frac{p+1}{2} \equiv \frac{p-1}{2}$, $-\frac{p+3}{2} \equiv \frac{p-3}{2}$, $\ldots$, $-(p-1) \equiv 1 \bmod p$, then we have introduced exactly $\frac{p-1}{2}$ factors -1; thus $(p-1)! \equiv (-1)^{(p-1)/2} a^2 \bmod p$ with $a = (\frac{p-1}{2})!)$. This proved the claim. ☐

Now we can prove Proposition 5.2: if $p \equiv 1 \bmod 4$, then we have just constructed a solution of the congruence $a^2 \equiv -1 \bmod p$, so assume conversely that this congruence is solvable. Raising both sides to the $\frac{p-1}{2}$-th power gives $1 \equiv a^{p-1} \equiv (-1)^{(p-1)/2} \bmod p$, and since $1 \not\equiv -1 \bmod p$ for odd primes p, we must have $(-1)^{(p-1)/2} = 1$, hence $p \equiv 1 \bmod 4$.

The solvability of $x^2 \equiv -1 \bmod p$ is the first of two steps in our proof of the Theorem of Girard-Fermat; the second one is a result due to Birkhoff, rediscovered by Aubry, and named after Thue:

Proposition 5.5. *Given an integer a not divisible by p, there exist $x, y \in \mathbb{Z}$ with $0 < |x|, |y| < \sqrt{p}$ such that $ay \equiv x \bmod p$.*

Proof. Let f be the smallest integer greater than $\sqrt{p}$, and consider the residue classes $\{[u + av] : 0 \le u, v < f\}$ modulo p. There are $f^2 > p$ such expressions, but only p different residue classes, hence there must exist u, u', v, v' such that $u + av \equiv u' + av' \bmod p$. Put $x = u - u'$ and $y = v' - v$; then $x \equiv ay \bmod p$, and moreover $-f < x, y < f$. □

Now we can prove

Theorem 5.6 (Girard-Fermat-Euler). *Every prime $p \equiv 1 \bmod 4$ is a sum of two integral squares.*

Proof. Since $p \equiv 1 \bmod 4$, there is an $a \in \mathbb{Z}$ such that $a^2 \equiv -1 \bmod 4$. By Thue's result, there are integers x and y such that $ay \equiv x \bmod p$ and $0 < x, y < \sqrt{p}$. Squaring gives $-y^2 \equiv x^2 \bmod p$, that is, $x^2 + y^2 \equiv 0 \bmod p$. Since $0 < x^2, y^2 < p$, we find $0 < x^2 + y^2 < 2p$; since $x^2 + y^2$ is divisible by p, we must have $x^2 + y^2 = p$. □

5.2 Quadratic Equations

Next we will apply the Unique Factorization Theorem to the solution of the diophantine equation

$$x^2 + y^2 = z^2$$

in integers $x, y, z \in \mathbb{Z}$. Such triples of solutions are called Pythagorean[3] triples. The most famous of these triples is of course $(3, 4, 5)$. It is quite easy to give formulas for producing such triples: for example, take $x = 2mn$, $y = m^2 - n^2$ and $z = m^2 + n^2$ (special cases were known to the Babylonians, the general case occurs in Euclid). It is less straightforward to verify that there are no other solutions (this was first done by the Arabs in the 10th century).

Assume that (x, y, z) is a Pythagorean triple. If d divides two of these, it divides the third, and then $(x/d, y/d, z/d)$ is another Pythagorean triple. We may therefore assume that x, y and z are pairwise coprime; such triples are called primitive. In particular, exactly one of them is even.

Claim 1. The even integer must be one of x or y. In fact, if z is even, then x and y are odd. Writing $x = 2X + 1$, $y = 2Y + 1$ and $z = 2Z$, we find $4X^2 + 4X + 4Y^2 + 4Y + 2 = 4Z^2$: but the left hand side is not divisible by 4: contradiction.

Exchanging x and y if necessary we may assume that x is even. Now we transfer the additive problem $x^2 + y^2 = z^2$ into a multiplicative one (if we are to use unique factorization, we need products, not sums) by writing $x^2 = z^2 - y^2 = (z - y)(z + y)$.

Claim 2. $\gcd(z - y, z + y) = 2$. In fact, put $d = \gcd(z - y, z + y)$. Then d divides $z - y$ and $z + y$, hence their sum $2z$ and their difference $2y$. Now

[3] Pythagoras of Samos (ca. 569 – 475 BC.).

$\gcd(2y, 2z) = 2\gcd(y, z) = 2$, so $d \mid 2$; on the other hand, $2 \mid d$ since $z - y$ and $z + y$ are even since z and y are odd. Thus $d = 2$ as claimed.

This is the point where Unique Factorization comes in:

Proposition 5.7. *Let $a, b \in \mathbb{N}$ be coprime integers such that ab is a square. Then a and b are squares.*

Proof. Write down the prime factorizations of a and b as

$$a = p_1^{a_1} \cdots p_r^{a_r}, \quad b = q_1^{b_1} \cdots q_s^{b_s}.$$

Now a and b are coprime, so the set of p_i and the set of q_j are disjoint, and we conclude that the prime factorization of ab is given by

$$ab = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s}.$$

Since ab is a square, all the exponents in the prime factorization of ab must be even. This implies that the a_i and the b_j are even, therefore a and b are squares. $\square$

Corollary 5.8. *Let $a, b \in \mathbb{N}$ be integers with $\gcd(a, b) = d$ such that ab is a square. Then a/d and b/d are squares.*

Proof. Apply the proposition to the pair a/d and b/d. $\square$

Applying the corollary to the case at hand (and observing that $z - y \in \mathbb{N}$, since $z + y > 0$ and $(z - y)(z + y) = x^2 > 0$) we find that there exist $m, n \in \mathbb{N}$ such that $z - y = 2n^2$ and $z + y = 2m^2$. Adding and subtracting these equations gives $z = m^2 + n^2$ and $y = m^2 - n^2$, and from $x^2 = (z - y)(z + y) = m^2n^2$ and $x \in \mathbb{N}$ we deduce that $x = 2mn$.

Note that we must have $\gcd(m, n) = 1$: in fact, any common divisor of m and n would divide x, y and z contradicting our assumption that our triple be primitive. We have shown:

Theorem 5.9. *If (x, y, z) is a primitive Pythagorean triple with x even, then there exist coprime integers $m, n \in \mathbb{N}$ such that $x = 2mn$, $y = m^2 - n^2$ and $z = m^2 + n^2$.*

Note that if y is even, then the general solution is given by $x = m^2 - n^2$, $y = 2mn$ and $z = m^2 + n^2$. Moreover, if we drop the condition that the triples be primitive then the theorem continues to hold if we also drop the condition that the integers m, n be relatively prime.

Lagrange's Trick

The same technique we used for solving $x^2 + y^2 = z^2$ can be used to solve equations of the type $x^2 + ay^2 = z^2$: just write the equation in the form $ay^2 = (z - x)(z + x)$ and use unique factorization.

Equations like $x^2 + y^2 = 2z^2$ at first seem intractable using this approach because we can't produce a difference of squares. Lagrange, however, saw that in this case multiplication by 2 saves the day because $(2z)^2 = 2x^2 + 2y^2 = (x+y)^2 + (x-y)^2$, hence $(2z - x - y)(2z + x + y) = (x-y)^2$, and now the solution proceeds exactly as for Pythagorean triples.

Let us now show that we can do something similar for any equation of type $AX^2 + BY^2 = CZ^2$ having at least one solution. First, multiplying through by A shows that it is sufficient to consider equations $X^2 + aY^2 = bZ^2$. Assume that (x, y, z) is a solution of this equation. Then

$$\begin{aligned}(bzZ)^2 &= bz^2X^2 + abz^2Y^2 \\ &= (x^2 + ay^2)X^2 + (ax^2 + a^2y^2)Y^2 \\ &= (xX + ayY)^2 + a(yX - xY)^2.\end{aligned}$$

Thus $a(yX - xY)^2 = (bzZ)^2 - (xX + ayY)^2$ is a difference of squares, and we can proceed as for Pythagoren triples. We have proved:

Theorem 5.10. *If the equation $ax^2 + by^2 = cz^2$ has a nontrivial solution in integers, then this equation can be factored over the integers (possibly after multiplying through by a suitable integer).*

5.3 Fermat's Last Theorem for Exponent 4

The solution of $x^2 + y^2 = z^2$ will help us prove that the diophantine equation

$$X^4 + Y^4 = Z^4 \tag{5.1}$$

has only trivial solutions, namely those with $X = 0$ or $Y = 0$. As a matter of fact, it is a lot easier to prove more, namely that

$$X^4 + Y^4 = Z^2 \tag{5.2}$$

has only trivial solutions (this *is* more: if $X^4 + Y^4$ cannot be a square, it cannot be a fourth power). The proof is quite involved and uses a technique that Fermat called infinite descent.

In a nutshell, the idea behind infinite descent is the following: if we want to prove that a certain diophantine equation is impossible in $\mathbb{N}$, it is sufficient to show that for every solution in natural numbers there is another solution that is "smaller", which eventually leads to a contradiction because there is no natural number smaller than 1.

Fermat used this idea to give a proof of

Theorem 5.11. *The Fermat equation* (5.2) *for the exponent* 4 *does not have any integral solution with $XYZ \neq 0$.*

Proof. Assume that $X, Y, Z \in \mathbb{N} \setminus \{0\}$ satisfy (5.2); we may (and will) assume that these integers are pairwise coprime (otherwise we can cancel common divisors). Now we vaguely follow our solution of the Pythagorean equation: Z must be odd (if Z were even, then X and Y would have to be odd, and we get a contradiction as in the proof of Theorem 5.9).

Thus we may assume that X is odd and Y is even. Since (X^2, Y^2, Z) is a Pythagorean Triple, there exist integers m, n such that $X^2 = m^2 - n^2$, $Y^2 = 2mn$ and $Z = m^2 + n^2$. Clearly $\gcd(m, n)$ divides both X and Y, hence m and n are coprime; moreover, since X is odd, we have $1 \equiv X^2 = m^2 - n^2 \bmod 4$, which implies that m is odd and $n = 2k$ is even. Thus $(Y/2)^2 = mk$ with m and k coprime, hence $m = a^2$ and $k = b^2$, giving $X^2 = a^4 - 4b^4$.

Now we repeat the trick: from $X^2 + 4b^4 = a^4$ we see that $(X, 2b^2, a^2)$ is a Pythagorean triple; thus $X = m_1^2 - n_1^2$, $2b^2 = 2m_1n_1$ and $a^2 = m_1^2 + n_1^2$, where m_1 and n_1 are (necessarily coprime) positive integers. From $m_1n_1 = b^2$ we deduce that $m_1 = r^2$ and $n_1 = s^2$, hence $a^2 = r^4 + s^4$, and we have found a new solution (a, r, s) to our equation $Z^2 = X^4 + Y^4$.

Since $Z = m^2 + n^2 = a^4 + 4b^4$, we find that $0 < a < Z$; this means that for every solution (X, Y, Z) in natural numbers there exists another solution with a smaller Z. This is impossible, so there can't be a nontrivial solution to the Fermat equation in the first place. $\square$

Exercises

5.1 Solve the diophantine equation $x^2 + 2y^2 = z^2$.

5.2 Solve the diophantine equation $x^2 - 2y^2 = z^2$.

5.3 Solve the diophantine equation $x^2 + y^2 = 2z^2$.

5.4 Solve the diophantine equation $x^2 - y^2 = 3$.

5.5 Prove that each odd prime p can be written as a difference of squares of natural numbers ($p = y^2 - x^2$ for $x, y \in \mathbb{N}$) in a unique way.

5.6 Fermat repeatedly challenged English mathematicians by sending them problems he claimed to have solved and asking for proofs. Two of them were the following that he sent to Wallis:

- Prove that the only solution of $x^2 + 2 = y^3$ in positive integers is given by $x = 5$ and $y = 3$;
- Prove that the only solution of $x^2 + 4 = y^3$ in positive integers is given by $x = 11$ and $y = 5$.

In a letter to his English colleague Digby, Wallis called these problems trivial and useless, and mentioned a couple of problems that he claimed were of a similar nature:

- $x^2 + 12 = y^4$ has unique solution $x = 2$, $y = 2$ in integers;
- $x^4 + 9 = y^2$ has unique solution $x = 2$, $y = 5$ in integers;
- $x^3 - y^3 = 20$ has no solution in integers;
- $x^3 - y^3 = 19$ has unique solution $x = 3$, $y = 2$ in integers.

When Fermat learned about Wallis's comments, he called Wallis's problems mentioned above "amusements for a three-day arithmetician" in a letter to Digby. In fact, while Fermat's problems were hard (and maybe even not solvable using the mathematics known in his times), Wallis's claims are easy to prove. Do this.

5.7 Assume that $ab = rx^n$ for $a, b, r, x \in \mathbb{N}$ and $\gcd(a, b) = 1$. Show that there exist $u, v, y, z \in \mathbb{N}$ such that $a = uy^n$, $b = vz^n$, and $uv = r$.

Chapter 6

Residue Class Rings

In the last chapter we have defined congruences and congruence classes, and we have shown that $\mathbb{Z}/m\mathbb{Z}$ forms a ring. Given any ring R, we can define its unit group $R^\times = \{u \in R : uv = 1 \text{ for some } v \in R\}$: this is the set of all elements dividing 1, or, equivalently, that have an inverse in R.

We have already seen that the unit group of $\mathbb{Z}$ is simply $\mathbb{Z}^\times = \{-1, +1\}$, a group of order 2. Let us now determine the unit groups of the rings of residue classes $\mathbb{Z}/m\mathbb{Z}$. Observe that a residue class $[u]_m$ modulo m is a unit if there exists an integer v such that $[uv]_m = [1]_m$, in other words: if $uv \equiv 1 \bmod m$ for some $v \in \mathbb{Z}$.

Now we claim

Theorem 6.1. *We have* $(\mathbb{Z}/m\mathbb{Z})^\times = \{a \bmod m : \gcd(a, m) = 1\}$.

Proof. It is now that the Bezout representation begins to show its full power. If $\gcd(a, m) = 1$, then there exist integers $x, y \in \mathbb{Z}$ such that $ax + my = 1$. Reducing this equation modulo m gives $ax \equiv 1 \bmod m$, in other words: the residue class $a \bmod m$ is a unit! Not only that: the extended Euclidean algorithm gives us a method to compute the inverse elements.

To prove the converse, assume that $a \bmod m$ is a unit. Then $ac \equiv 1 \bmod m$ for some $c \in \mathbb{Z}$, so $ac = km + 1$ for some $k \in \mathbb{Z}$. But then $ac - km = 1$ shows that $\gcd(a, m) = 1$. □

If $m = p$ is a prime, the unit groups are particularly simple: we have $\gcd(a, p) = 1$ if and only if $p \nmid a$, hence $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \ldots, p-1\} = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$. But if every element $\neq 0$ of a ring has an inverse, then that ring is a field, and we have proved

Corollary 6.2. *If p is a prime, then the residue class ring $\mathbb{Z}/p\mathbb{Z}$ is a field.*

The field $\mathbb{Z}/p\mathbb{Z}$ is called a finite field because it has finitely many elements. As we have seen, there are finite fields with p elements for every prime p. Later we will see that there exist finite fields with $m > 1$ elements if and only if m is a prime power.

The fact that $\mathbb{Z}/p\mathbb{Z}$ is a field means that expressions like $\frac{1}{7} \bmod 11$ make sense. To compute such 'fractions', you can choose one of the following two methods:

1. Change the numerator mod 11 until the division becomes possible:
$$\frac{1}{7} \equiv \frac{12}{7} \equiv \frac{23}{7} \equiv \frac{34}{7} \equiv \frac{45}{7} \equiv \frac{56}{7} = 8 \bmod 11,$$
and in fact $7 \cdot 8 = 56 \equiv 1 \bmod 11$. This method only works well if p is small.

2. Apply the Euclidean algorithm to the pair $(7, 11)$, and compute a Bezout representation; you will find that $1 = 2 \cdot 11 - 3 \cdot 7$, and reducing mod 11 gives $1 \equiv (-3) \cdot 7 \bmod 11$, hence the multiplicative inverse of 7 mod 11 is $-3 \equiv 8 \bmod 11$.

6.1 Euler-Fermat

Theorem 6.3 (Fermat's Little Theorem). *If p is a prime and a an integer not divisible by p, then $a^{p-1} \equiv 1 \bmod p$.*

The following proof is due to Leibniz[1] and probably the oldest proof known for Fermat's Little Theorem. It uses binomial coefficients: these are the entries in Pascal's triangle, and they occur in the binomial theorem
$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-1}ab^{n-1} + b^n.$$
We will need two properties of $\binom{n}{k}$: first we use the formula $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ (which was how we defined them in Chapter 3), and then we claim

Lemma 6.4. *If p is a prime, then the numbers $\binom{p}{k}$, $k = 1, 2, \ldots, p-1$, are all divisible by p.*

For example, the fifth row of Pascal's triangle is 1 5 10 10 5 1. The claim is not true if p is not a prime: the sixth row is 1 6 15 20 15 6 1, and the numbers 15 and 20 are not divisible by 6.

Proof. From $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ we see that the numerator is divisible by p while the denominator is not divisible by p unless $k = 0$ or $k = p$. Thus we conclude that $p \mid \binom{p}{k}$ for $0 < k < p$. □

Now we can give an induction proof of Fermat's Little Theorem:

[1] Gottfried Wilhelm von Leibniz, 1646 (Leipzig) – 1716 (Hannover).

Proof. We prove the equivalent (!) statement $a^p \equiv a \bmod p$ for all $a \in \mathbb{Z}$ via induction on a. The claim is clearly trivial for $a = 1$; assume it has been proved for some a; then

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \ldots + \binom{p}{p-1} a + 1.$$

Since the binomial coefficients are all $\equiv 0 \bmod p$ by the lemma, we find

$$(a+1)^p \equiv a^p + 1 \bmod p,$$

and by the induction assumption, $a^p \equiv a \bmod p$, so we get $(a+1)^p \equiv a+1 \bmod p$, and the induction step is established. $\square$

There is another proof of Fermat's little theorem that works for any finite group. To see what's going on, consider $(\mathbb{Z}/5\mathbb{Z})^\times = \{[1],[2],[3],[4]\}$, where $[r]$ denotes the residue class $r \bmod 5$. If we multiply each of these classes by 3, we get

$$\begin{aligned} [1]\cdot[3] &= [3], \\ [2]\cdot[3] &= [1], \\ [3]\cdot[3] &= [4], \\ [4]\cdot[3] &= [4]; \end{aligned}$$

thus multiplying all prime residue classes mod 5 by 3 yields the same classes again, though in a different order. If we multiply these four equations together, we get $[1][2][3][4]\cdot[3]^4 = [3][1][4][2] = [1][2][3][4]$, hence $[3]^4 = [1]$, or, in other words, $3^4 \equiv 1 \bmod 5$. This can be done in general:

Second Proof of Thm. 6.3. Write $(\mathbb{Z}/p\mathbb{Z})^\times = \{[1],[2],\ldots,[p-1]\}$; let a be an integer not divisible by p. If we multiply each residue class with $[a]$, we get the $p-1$ classes $[a]$, $[2a]$, …, $[(p-1)a]$:

$$\begin{aligned} [1]\cdot[a] &= [a] \\ [2]\cdot[a] &= [2a] \\ &\vdots \\ [p-1]\cdot[a] &= [(p-1)a] \end{aligned}$$

If we can show that the classes on the right hand side are all different, then they must be a permutation of the classes $[1]$, …, $[p-1]$ that we started with. Taking this for granted, the products $[a]\cdot[2a]\cdots[(p-1)a] = [(p-1)!][a^{p-1}]$ and $[1]\cdot[2]\cdots[p-1] = [(p-1)!]$ must be equal (after all, the factors are just rearranged). But $(p-1)!$ is coprime to p, so we may cancel this factor, and get $[a^{p-1}] = [1]$, i.e., $a^{p-1} \equiv 1 \bmod p$.

It remains to show that the classes $[a]$, $[2a]$, …, $[(p-1)a]$ are all different. Assume therefore that $[ra] = [sa]$ for integers $1 \le r, s \le p-1$; we have to show that $r = s$. But $[ra] = [sa]$ means that $[(r-s)a] = [0]$, i.e. that $p \mid (r-s)a$. Since $p \nmid a$ by assumption, the fact that p is prime implies $p \mid (r-s)$. But $r-s$ is an integer strictly between $-p$ and p, and the only such integer is 0: thus $r = s$ as claimed. $\square$

Assume that we are given an integer m and an integer a coprime to m. The smallest exponent $n > 0$ such that $a^n \equiv 1 \bmod m$ is called the order of $a \bmod m$; we write $n = \operatorname{ord}_m(a)$. Note that we always have $\operatorname{ord}_m(1) = 1$. Here's a table for the orders of elements in $(\mathbb{Z}/7\mathbb{Z})^\times$:

$a \bmod 7$	1	2	3	4	5	6
$\operatorname{ord}_7(a)$	1	3	6	3	6	2

If $m = p$ is prime, then Fermat's Little Theorem gives us $a^{p-1} \equiv 1 \bmod p$, i.e., the order of $a \bmod p$ is at most $p-1$. In general, the order of a is not $p-1$; it is, however, always a divisor of $p-1$ (as the table above suggested):

Proposition 6.5. *Given a prime p and an integer a coprime to p, let n denote the order of a modulo p. If m is any integer such that $a^m \equiv 1 \bmod p$, then $n \mid m$. In particular, n divides $p-1$.*

Proof. Write $d = \gcd(n, m)$ and $d = nx + my$; then $a^d = a^{nx+my} \equiv 1 \bmod p$ since $a^n \equiv a^m \equiv 1 \bmod p$. The minimality of n implies that $n \le d$, but then $d \mid n$ shows that we must have $d = n$, hence $n \mid m$. $\square$

Here comes a pretty application to prime divisors of Mersenne and Fermat numbers.

Corollary 6.6. *If p is an odd prime and if $q \mid M_p$, then $q \equiv 1 \bmod 2p$.*

Proof. It suffices to prove this for prime values of q (why?). So assume that $q \mid 2^p - 1$; then $2^p \equiv 1 \bmod q$. By Proposition 6.5, the order of $2 \bmod p$ divides p, and since p is prime, we find that $p = \operatorname{ord}_p(a)$.

On the other hand, we also have $2^{q-1} \equiv 1 \bmod p$ by Fermat's little theorem, so Proposition 6.5 gives $p \mid (q-1)$, and this proves the claim because we clearly have $q \equiv 1 \bmod 2$. $\square$

Example: $M_{11} = 2047 = 23 \cdot 89$.

Fermat numbers are integers $F_n = 2^{2^n} + 1$ (thus $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$, ...), and Fermat conjectured (and once even seemed to claim he had a proof) that these integers are all primes. These integers became much more interesting when Gauss succeeded in proving that a regular p-gon, p an odd prime, can be constructed with ruler and compass if p is a Fermat prime. Gauss also stated that he had proved the converse, namely that if a regular p-gon can be constructed by ruler and compass, then p is a Fermat prime, but the first (almost) complete proof was given by Pièrre Wantzel.[2]

[2]Pièrre Wantzel, 1814 (Paris) – 1848 (Paris).

Corollary 6.7. *If q divides F_n, then $q \equiv 1 \bmod 2^{n+1}$.*

Proof. It is sufficient to prove this for prime divisors q. Assume that $q \mid F_n$; then $2^{2^n} + 1 \equiv 1 \bmod q$, hence $2^{2^n} \equiv -1 \bmod q$ and $2^{2^{n+1}} \equiv 1 \bmod q$. We claim that actually $2^{n+1} = \operatorname{ord}_q(2)$: in fact, Proposition 6.5 says that the order divides 2^{n+1}, hence is a power of 2. But 2^{n+1} is clearly the smallest power of 2 that does it.

On the other hand, $2^{q-1} \equiv 1 \bmod q$ by Fermat's Little Theorem, and Proposition 6.5 gives $2^{n+1} \mid (q-1)$, which proves the claim. ☐

In particular, the possible prime divisors of $F_5 = 4294967297$ are of the form $q = 64m + 1$. After a few trial divisions one finds $F_5 = 641 \cdot 6700417$. This is how Euler disproved Fermat's conjecture. Today we know the prime factorization of F_n for all $n \le 11$, we know that F_n is composite for $5 \le n \le 30$ (and several larger values up to $n = 382447$), and we don't know any factors for $n = 14, 20, 22$ and 24. See
`http://vamri.xray.ufl.edu/proths/fermat.html`
for more.

Euler's Theorem

Consider the unit group $(\mathbb{Z}/15\mathbb{Z})^\times$ of $\mathbb{Z}/15\mathbb{Z}$. It consists of the eight residue classes [1], [2], [4], [7], [8], [11], [13], [14]. If we multiply each of these classes e.g. by [7] (or [8], [9]), then we get

$$\begin{array}{rcrrcrrcr}
[1]\cdot[7] & = & [7] & [1]\cdot[8] & = & [8] & [1]\cdot[9] & = & [9] \\
[2]\cdot[7] & = & [14] & [2]\cdot[8] & = & [1] & [2]\cdot[9] & = & [3] \\
[4]\cdot[7] & = & [13] & [4]\cdot[8] & = & [2] & [4]\cdot[9] & = & [6] \\
[7]\cdot[7] & = & [4] & [7]\cdot[8] & = & [11] & [7]\cdot[9] & = & [3] \\
[8]\cdot[7] & = & [11] & [8]\cdot[8] & = & [4] & [8]\cdot[9] & = & [12] \\
[11]\cdot[7] & = & [2] & [11]\cdot[8] & = & [13] & [11]\cdot[9] & = & [9] \\
[13]\cdot[7] & = & [1] & [13]\cdot[8] & = & [14] & [13]\cdot[9] & = & [12] \\
[14]\cdot[7] & = & [8] & [14]\cdot[8] & = & [7] & [14]\cdot[9] & = & [6]
\end{array}$$

As in our proof of Fermat's Little Theorem, the resulting residue classes (for multiplication by [7] and [8]) are the classes we started with in a different order. Multiplying these equations we get

$$\prod_{(a,15)=1} [a] = \prod_{(a,15)=1} [7a] = [7]^8 \prod_{(a,15)=1} [a].$$

Since the a are coprime to 15, so is their product; thus we may cancel, and we find $[7]^8 = [1]$, or $7^8 \equiv 1 \bmod 15$. Similarly, we find $8^8 \equiv 1 \bmod 15$; for multiplication by 9, however, the classes on the right hand side differ from those on the left (they're all divisible by 3 since both 9 and 15 are), and we do *not* get $9^8 \equiv 1 \bmod 15$.

The same idea works in general. Let $m \ge 2$ be an integer, and let $\phi(m)$ denote the number of residue classes coprime to m, that is, $\varphi(m) = \#(\mathbb{Z}/m\mathbb{Z})^\times$.

Then we have the following result, which is usually referred to as the Euler-Fermat Theorem: it is due to Euler, but contains Fermat's Little Theorem as a special case.

Theorem 6.8. *If a is an integer coprime to $m \geq 2$, then $a^{\varphi(m)} \equiv 1 \bmod m$.*

For $m = p$ prime, we have $\phi(p) = p - 1$, and Euler's Theorem becomes Fermat's Little Theorem.

Proof. Let $[r_i]$, $i = 1, \ldots, t = \phi(m)$, denote the residue classes in $(\mathbb{Z}/m\mathbb{Z})^\times$. Then we claim that $[ar_1]$, …, $[ar_t]$ are pairwise distinct. In fact, assume that $[ar_i] = [ar_j]$ with $i \neq j$, that is, $ar_i \equiv ar_j \bmod m$. Since $\gcd(a, m) = 1$, we may cancel a, and get $[r_i] = [r_j]$: contradiction.

Since the classes $[ar_1]$, …, $[ar_t]$ are all in $(\mathbb{Z}/m\mathbb{Z})^\times$ and different, and since there are only t different classes in $(\mathbb{Z}/m\mathbb{Z})^\times$, we must have $(\mathbb{Z}/m\mathbb{Z})^\times = \{[ar_1], \ldots, [ar_t]\}$. But then $\prod_{i=1}^t [r_i] = \prod_{i=1}^t [ar_i] = [a]^{\phi(m)} \prod_{i=1}^t [r_i]$. Since the $[r_i]$ are coprime to m, so is their product. Cancelling then gives $[a]^{\phi(m)} = [1]$, which proves the claim. $\square$

6.2 Euler's Phi Function

For the application of Euler-Fermat we need a formula that allows us to compute $\phi(n)$. Let us first compute $\phi(n)$ directly for some small n. For $n = 6$, there are 6 different residue classes modulo 6; the classes [0], [2], [3] and [4] are not coprime to 6 (or, in other words, do not have a multiplicative inverse), which leaves the classes [1] and 5 as the only ones that are coprime to 6: thus $\phi(6) = 2$. The classes mod 8 coprime to 8 are [1], [3], [5], [7], hence $\phi(8) = 4$. If p is prime, then all the $p-1$ classes [1], [2], …, $[p-1]$ are coprime to p, hence $\phi(p) = p-1$.

n	3	4	5	6	7	8	9	10	12	15
$\phi(n)$	2	2	4	2	6	4	6	4	4	8

We can easily compute $\phi(p^k)$ (Euler's phi function for prime powers): starting with all the nonzero classes [1], [2], …, $[p^2 - 1]$ (there are $p^2 - 1$ of them) we have to eliminate those that are not coprime to p^2, that is, exactly the multiples of p smaller than p^2: these are p, $2p$, $3p$, …, $(p-1)p$ (note that $p \cdot p = p^2 > p^2 - 1$); since there are exactly $p - 1$ of these multiples of p, there will be exactly $p^2 - 1 - (p-1) = p^2 - p = p(p-1)$ classes left: thus $\phi(p^2) = p(p-1)$.

The same method works for p^k: there are exactly $p^k - 1$ nonzero classes, namely [1], [2], …, $[p^k - 1]$. The multiples of p among these classes are $[p]$, $[2p]$, …, $p^k - p = (p^{k-1} - 1)p$, and there are exactly $p^{k-1} - 1$ of them. Thus $\phi(p^k) = p^k - 1 - (p^{k-1} - 1) = p^k - p^{k-1} = p^{k-1}(p-1)$.

We have proved

Proposition 6.9. *For primes p and integers $k \geq 1$, we have*

$$\phi(p^k) = p^{k-1}(p-1).$$

Let us now compute $\phi(pq)$ for a product of two different primes. We have $pq - 1$ nonzero residue classes $[1]$, $[2]$, ..., $[pq-1]$. The classes that have a factor in common with pq are multiples of p and multiples of q, namely $[p]$, $[2p]$, ..., $[(q-1)p$ and $[q]$, $[2q]$, ..., $[(p-1)q]$. Since there are no multiples of p that are multiples of q (like $[0]$, $[pq]$, etc) among these, there will be exactly $pq - 1 - (p-1) - (q-1) = pq - p - q + 1 = (p-1)(q-1)$ classes left after eliminating multiples of p or q. Thus $\phi(pq) = (p-1)(q-1) = \phi(p)\phi(q)$.

The general result is

Proposition 6.10. *If m and n are coprime integers, then $\phi(mn) = \phi(m)\phi(n)$.*

Before we turn to the proof, let's see how it works in a specific example like $m = 5$ and $n = 3$. What we'll do is take a residue class modulo 15 and coprime to 15, and map it to a pair of residue classes mod 3 and mod 5:

a mod 15	1	2	4	7	8	11	13	14
a mod 3	1	2	1	1	2	2	1	2
a mod 5	1	2	4	2	3	1	3	4

Thus we have the following pairs of residue classes modulo 3 and 5: $(1,1)$, $(1,2)$, $(1,3)$, $(1,4)$ and $(2,1)$, $(2,2)$, $(2,3)$, $(2,4)$. In particular, there are $\phi(5) = 4$ pairs with $a \equiv 1 \bmod 3$ and 4 pairs with $a \equiv 2 \bmod 3$.

Proof of Prop. 6.10. We have to find a map sending a residue class modulo mn to two residue classes modulo m and n. Let's try

$$\psi : (\mathbb{Z}/mn\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times : [a]_{mn} \longmapsto ([a]_m, [a]_n).$$

All that's left to do is check that it works. First observe that $\gcd(ab, n) = 1$ if and only if $\gcd(a, n) = \gcd(b, n) = 1$.

Surjectivity: We have to show that, given residue classes $[r]_m$ and $[s]_n$, there exists a residue class $[a]_{mn}$ such that $[a]_m = [r]_m$ and $[a]_n = [s]_n$. At this point, Bezout comes in again: since $\gcd(m, n) = 1$, there exist $x, y \in \mathbb{Z}$ such that $1 = mx + ny$. Now put $a = ryn + sxm$: then $a = ryn + sxm \equiv ryn \equiv 1 \bmod m$ since $yn \equiv 1 \bmod m$ from the Bezout representation, and similarly $a = ryn + sxm \equiv sxm \equiv s \bmod n$.

Injectivity: Assume that there are residue classes $[a]_{mn}$ and $[b]_{mn}$ such that $[a]_m = [b]_m$ and $[a]_n = [b]_n$. Then $m \mid (b-a)$ and $n \mid (b-a)$, and since $\gcd(m, n) = 1$, this implies that $[a]_{mn} = [b]_{mn}$ and proves the injectivity of ϕ. $\square$

Proof 5 of the Infinitude of Primes. (Euler[3] 1849). Assume that there are only finitely many primes, and let D denote their product. Then

$$\phi(D) = \prod_p (p-1) \geq 2 \cdot 4 \cdots > 2,$$

[3] Leonhard Euler, 1707 (Basel, Switzerland) – 1783 (St. Petersburg, Russia).

hence there must be an integer a in the interval $[2, D]$ coprime to D. This a can't have any prime divisor and so must be equal to 1, which contradicts $a \geq 2$.

Again, if you take $a = D - 1$ you basically get back Euclid's proof with $N - 1$ instead of the original $N + 1$.

6.3 Primitive Roots

The main theorem of this section is the existence of primitive roots modulo primes p. Consider the residue classes [2] and [3] modulo 7. Then the classes represented by powers of [2] are [2], $[4] = [2]^2$, and $[1] = [2]^3$; these are half of the nonzero classes modulo 7. The powers of [3], on the other hand, are [3], $[2] = [3]^2$, $[6] = [3]^3$, $[4] = [3]^4$, $[5] = [5]^5$, and $[1] = [3]^6$, so the powers of [3] generate all the nonzero classes modulo 7. For this reason, we call 3 a primitive root modulo 7, whereas 2 is not a primitive root modulo 7.

Instead of proving that for every prime p there is a primitive root g, we shall prove a more general result:

Theorem 6.11. *The multiplicative group of a finite field is cyclic.*

For the proof we a bit of information on the order of elements a in finite abelian groups G: this is the smallest positive integer r such that $a^r = 1$.

Lemma 6.12. *If an element g of order n in some finite abelian group G. If $g^m = 1$, then $n \mid m$.*

Proof. Write $m = qn + r$ with $0 \leq r < n$ (Euclidean division); then $1 = g^m = g^{qn+r} = q^{qn}g^r = g^r$. Since n is the minimal positive exponent with this property and $r < n$, we must have $r = 0$. This proves the claim. □

Lemma 6.13. *If G is an abelian group, and if $a, b \in G$ are elements of order m and n respectively such that $\gcd(m, n) = 1$, then ab has order mn.*

Proof. Clearly $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^m)^n = 1$, so ab has order dividing mn (note that we have used commutativity here).

For the converse, let k denote the order of mn, that is the minimal integer k with $1 \leq k \leq mn$ such that $(ab)^k = 1$; we have to show that $k = mn$.

From $(ab)^k = 1$ we get $1 = (ab)^{km} = a^{km}b^{km} = b^{km}$; hence $n \mid km$ by Lemma 6.12; since $\gcd(n, m) = 1$, we have $n \mid k$.

Exactly the same reasoning with the roles of a and b interchanged shows that $m \mid k$. But $\gcd(m, n) = 1$, hence $n \mid k$ and $m \mid k$ imply that $mn \mid k$. Since $k \neq 0$, we conclude that $k \geq mn$, and this proves the claim. □

Finally, let us prove Lagrange's Theorem:

Proposition 6.14. *Let G be a finite abelian group with n elements. Then $g^n = 1$ for all $g \in G$.*

Proof. Let $g_1 = 1$, g_2, $\ldots$, g_n be the elements of G. We multiply each of these elements by g and get $g_i g = g_{\pi(i)}$ for some index $\pi(i) \in \{1, \ldots, n\}$. We claim that π permutes the indices, i.e., that the $g_{\pi(i)}$ are just the elements g_i in some (possibly) different order.

For this end, it suffices to show that the $g_{\pi(i)}$ are pairwise different: because then there are n such elements, and since G has only n elements, the claim follows. But assume that $g_i g = g_j g$; multiplying through by the inverse of g gives $g_i = g_j$, hence $i = j$.

Multiplying the equations $g_i g = g_{\pi(i)}$ together, we get $g^n \prod g_i = \prod g_{\pi(i)}$. Now π permutes the indices, hence $\prod g_i = \prod g_{\pi(i)}$; canceling gives $g^n = 1$. □

In the special case where G is the additive group $G = \mathbb{Z}/n\mathbb{Z}$, the result is trivial, since it says that $n[a] = [0]$ for any residue class $[a] \in \mathbb{Z}/n\mathbb{Z}$. If $G = (\mathbb{Z}/p\mathbb{Z})^\times$, however, then $\#G = p - 1$, and Lagrange's theorem says that $[a]^{p-1} = [1]$ for $a \in (\mathbb{Z}/p\mathbb{Z})^\times$: this is Fermat's Little Theorem. Finally, if $G = (\mathbb{Z}/m\mathbb{Z})^\times$, then $\#G = \phi(m)$, and Lagrange's theorem gives the theorem of Euler-Fermat.

Proof of Theorem 6.11. If $n = 1$, the claim is trivial. If $n > 1$, let p be a prime divisor of the order n of $F^\times$. Then there is an element $a \in F$ such that $a^{n/p} \neq 1$. For if not, then every $a \in F$ is a root of the polynomial $f(X) = X^{n/p} - 1$; in particular, f has degree n/p and n roots. But polynomials f over fields can have at most $\deg f$ roots: contradiction.

Now let p^r be the exact power of a prime p that divides $n = \#F^\times$; then we claim that the element $x = a^{n/p^r}$ has order p^r. In fact, $x^{p^r} = a^n = 1$ by Lagrange's Theorem (in the case that we are most interested in, namely $F = \mathbb{Z}/p\mathbb{Z}$, this is just Fermat's Little Theorem), so the order of x divides p^r by Lemma 6.12. If the order were smaller, then we would have $x^{p^{r-1}} = 1$; but $x^{p^{r-1}} = a^{n/p} \neq 1$ by choice of a.

Now write $n = p_1^{r_1} \cdots p_t^{r_t}$. By the above, we can construct an element x_i of order $p_i^{r_i}$ for every $1 \le i \le t$. But then $x_1 \cdots x_t$ has order n by Lemma 6.13 (use induction). □

The fact that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic can be used to give another proof of the fact that the congruence $x^2 \equiv -1 \bmod p$ is solvable if $p \equiv 1 \bmod 4$: since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, there is an element $g \in \mathbb{Z}$ such that $[x]$ has order $p - 1$. Thus $g^{p-1} \equiv 1 \bmod p$, hence $p \mid (g^{p-1} - 1) = (g^{(p-1)/2} - 1)(g^{(p-1)/2} + 1)$. If p divided the first factor, then $[g]$ would have order dividing $\frac{p-1}{2}$; thus p divides the second factor, and we find $g^{(p-1)/2} \equiv -1 \bmod p$. Put $x = g^{(p-1)/4}$; then $x^2 \equiv -1 \bmod p$.

Definition. We say that an integer g is a primitive root modulo m if the powers of g generate all residue classes coprime to m. For example, 3 is a primitive root modulo 7, but 2 is not.

Corollary 6.15. *For every prime p there exist primitive roots.*

Proof. Since $\mathbb{Z}/p\mathbb{Z}$ is a finite field, the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, that is, there exists an integer g of order $p-1$; the powers of g generate the whole group $(\mathbb{Z}/p\mathbb{Z})^\times$. □

Exercises

6.1 Compute the addition and multiplication tables for the ring $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and compare the result to those for $\mathbb{Z}/4\mathbb{Z}$.

6.2 Do the same exercise for the rings $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$.

Chapter 7

Applications

In this chapter we will indicate how the theory of congruences and finite fields can be applied to problems in factorization of integers, cryptography and coding theory.

7.1 RSA

Cryptography deals with methods that allow us to transmit information safely, that is, in such a way that eavesdroppers have no chance of reading it. Simple methods for encrypting messages were known and widely used in military circles for several millenia; basically all of these codes are easy to break with computers.

An example of such a classical code is Caesar's cipher: permute the letters of the alphabet by sending X $\longmapsto$ A, Y $\longmapsto$ B, Z $\longmapsto$ C, A $\longmapsto$ D etc; the text "ET TU, BRUTE" would be encrypted as "BQ QR, YORQB". For longer texts, analyzing the frequency of letters (for given languages) makes breaking this and similar codes a breeze, in particular if you are equipped with a computer.

Another common feature of these ancient methods of encrypting messages is the following: anyone who knows the key, that is, the method with which messages are encrypted, can easily break the code by inverting the encryption. In 1976, Diffie and Hellman suggested the existence of public key cryptography: these are methods for encrypting messages that do not allow you to read encrypted messages even if you know the key. The most famous of all public key cryptosystems is called RSA after its discoverers Ramir, Shamir and Adleman (1978).

Here's the simple idea: assume that Bob wants to receive secure messages; he selects two (large) primes p and q and forms their product $n = pq$. Bob also chooses an integer $E < n$ coprime to $(p-1)(q-1)$. The integers n and E are made public and constitute the key, so everybody can encrypt messages. For decrypting messages, however, one needs to know the prime factors p and q, and if p and q are large enough (say about 150 digits each) then known factorization methods cannot factor n in any reasonable amount of time (say 100 years).

How does the encryption work? It is a simple matter to transform any text into a sequence of numbers, for example by using $a \longmapsto 01$, $b \to 02$, $\ldots$, with a couple of extra numbers for blanks, commas, etc. We may therefore assume that our message is a sequence of integers $T < n$ (if the text is longer, break it up into smaller pieces). Alice encrypts each integer T as $C \equiv T^E \bmod n$ and sends the sequence of C's to Bob (by email, say). Now Bob can decrypt the message as follows: since he knows p and q, he can form the product $m = (p-1)(q-1)$ and run the Euclidean algorithm on the pair (E, m) to find an integer D such that $DE \equiv 1 \bmod m$. Now he takes the message C and computes $C^D \bmod n$. The result is $C^D \equiv (T^E)^D = T^{DE} \bmod n$, but since $DE \equiv 1 \bmod m = \phi(n)$, the theorem of Euler-Fermat shows that $C^D \equiv T \bmod n$, and Bob has got the original text that Alice sent him.

Now assume that Celia is eavesdropping. Of course she knows the pair (n, E) (which is public anyway), and she also knows the message C that Alice sent to Bob. That does not suffice for decrypting the message, however, since one seems to need an inverse D of $E \bmod (p-1)(q-1)$ to do that; it is likely that one needs to know the factors of n in order to compute D.

Baby Example. The following choice of $n = 1073$ with $p = 29$ and $q = 37$ is not realistic because this number can be factored easily; its only purpose is to illustrate the method.

So assume that Bob picks the key $(n, E) = (1073, 25)$. Alice wants to send the message "miss piggy" to Bob. She starts by transforming the message into a string of integers as follows:

	m	i	s	s		p	i	g	g	y
T	13	9	19	19	27	16	9	7	7	25

Next she encrypts this sequence by computing $C \equiv T^{25} \bmod n$ for each of these T: starting with $13^{25} \equiv 671 \bmod 1073$, she finds

T	13	9	19	19	27	16	9	7	7	25
C	671	312	901	901	656	1011	312	922	922	546

Alice sends this string of C's to Bob. Knowing the prime factorization of n, Bob is able to compute the inverse of $25 \bmod (p-1)(q-1)$ as follows: he multiplies $p - 1 = 28$ and $q - 1 = 36$ to get $(p-1)(q-1) = 28 \cdot 36 = 1008$. Then he applies the extended Euclidean algorithm to $(25, 1008)$ and finds $1 = 25 \cdot 121 - 1008 \cdot 3$, and this shows that $D = 121$.

Now Bob takes the string of C's he got from Alice and decrypts them: starting with $671^{121} \equiv 13 \bmod n$ he can get back the string of T's, and hence the original message.

Remark. There is a big problem with this baby example: if we encrypt the message letter for letter, then equal letters will have equal code, and the cryptosystem can be broken (if the message is long enough) by analyzing the frequency with which each letter occurs (say in English). This problem vanishes into thin air when we use (realistic) key sizes of about 200 digits: there we encrypt the message in blocks of about 100 letters, and since the chance that any two blocks of 100 letters inside a message coincide is practically 0, an attack based on the frequency of letters will not be successful for keys of this size.

RSA can also be applied to the signature problem. Assume that Alice receives an email from someone claiming to be Bob. How can Alice verify that this is true? Here's the simple trick in a nutshell: both Bob and Alice choose public keys, say (n_A, E_A) for Alice and (n_B, E_B) for Bob. Moreover, Alice knows D_A with $D_A E_A \equiv 1 \bmod \phi(n_A)$, while Bob knows D_B with $D_B E_B \equiv 1 \bmod \phi(n_B)$. Now Bob encrypts his message as above, but instead of sending the T's to Alice, he computes $U = T^{D_B} \bmod n_B$ and sends the U's. In order to decrypt the message, Alice computes first $T \equiv U^{E_D} \bmod n_B$ and then decrypts the T's as in the original version of RSA using her D_A. If this works, then Alice can be sure that the message came from Bob because in order to encrypt the message this way, the sender has to know D_B.

7.2 Flannery's Cayley-Purser Algorithm

There are many public key cryptosystems; the general idea is to replace the group $(\mathbb{Z}/n\mathbb{Z})^\times$ used in RSA by other finite groups. The following algorithm was proposed by Sarah Flannery in connection with a school project she took part in and earned her the title Irish Young Scientist of the Year 1999 (check out her book).

In this system, $(\mathbb{Z}/n\mathbb{Z})^\times$ is replaced by its 2-dimensional analogue, the group $\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$. In general, $\mathrm{GL}(k, \mathbb{Z}/n\mathbb{Z})$ is the group of all $k \times k$-matrices A with entries in $\mathbb{Z}/n\mathbb{Z}$ whose determinant $d = \det A$ satisfies $\gcd(d, n) = 1$. If this condition holds, then the well known formulas for inverting A still make sense, hence such matrices have inverses: there exist $B \in \mathrm{GL}(k, \mathbb{Z}/n\mathbb{Z})$ such that $AB = 1$, where 1 is the matric having 1 on the diagonal and 0 everywhere else.

For $k = 1$, the matrices are 1×1-matrices, i.e., numbers $A = (a)$, and the condition $\gcd(\det A, n) = 1$ boils down to $\gcd(a, n) = 1$.

One of the key observations for RSA was the theorem of Euler-Fermat, and in this connection the fact that $\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$ played a central role. Note that $\phi(n)$ is the order of the group $\mathrm{GL}(1, \mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^\times$.

What is the order of the group $\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$ for $n = pq$?

Lemma 7.1. *Let $n = pq$ be the product of two distinct primes. Then $\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$ has exactly $n\phi(n)^2(p+1)(q+1)$ elements.*

Proof. Consider the map $\pi : \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z}) \longrightarrow \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z}) \times \mathrm{GL}(2, \mathbb{Z}/q\mathbb{Z})$ defined by

$$\begin{pmatrix} [a]_n & [b]_n \\ [c]_n & [d]_n \end{pmatrix} \longmapsto \left(\begin{pmatrix} [a]_p & [b]_p \\ [c]_p & [d]_p \end{pmatrix}, \begin{pmatrix} [a]_q & [b]_q \\ [c]_q & [d]_q \end{pmatrix} \right).$$

Using the Chinese remainder theorem it is not too hard to show that π is bijective (even an isomorphism). This means that

$$\#\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z}) = \#\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z}) \times \#\mathrm{GL}(2, \mathbb{Z}/q\mathbb{Z}).$$

Thus it remains to count the number of elements in $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$.

We have $p^2 - 1$ choices for the first column (every vector except the zero vector will do). The second column has to be independent from the first; there are p multiples of the first column vector, which means that we have $p^2 - p$ choices for the second vector. Thus there are $(p^2-1)(p^2-p) = p(p-1)^2(p+1)$ matrices with entries in $\mathbb{Z}/p\mathbb{Z}$ and nonzero determinant. $\square$

Just as in RSA, if Alice wants to receive messages, she has to come up with a public key. She picks two (large) primes p, q and computes $n = pq$. Then she picks (randomly) matrices $\alpha, \chi \in GL(2, \mathbb{Z}/n\mathbb{Z})$ such that $\chi\alpha^{-1} \neq \alpha\chi$, and computes $\beta = \chi^{-1}\alpha\chi$ and $\gamma = \chi^r$ for some fixed integer $r \in \mathbb{N}$.

The public key consists of n, α, β, γ.

Now Bob can send messages μ to Alice:

- he picks a random integer s,
- computes $\delta = \chi^s$,
- $\varepsilon = \delta^{-1}\alpha\delta$,
- $\kappa = \delta^{-1}\beta\delta$.

Now μ is enciphered by $\mu' = \kappa\mu\kappa$, and Bob sends μ' and ε to Alice.

When Alice receives (μ', ε), she computes $\lambda = \chi^{-1}\varepsilon\chi$ and then $\mu = \lambda\mu'\lambda$ is the plain text.

Why? Well, because

$$\begin{array}{rcll} \lambda & = & \chi^{-1}\varepsilon\chi \;=\; \chi^{-1}(\delta^{-1}\alpha\delta)\chi & \\ & = & \delta^{-1}(\chi^{-1}\alpha\chi)\delta & \chi \text{ commutes with } \delta = \chi^{rs} \\ & = & \delta^{-1}(\chi^{-1}\alpha^{-1}\chi)^{-1}\delta \;=\; \delta^{-1}\beta^{-1}\delta & \text{since } \beta = \chi^{-1}\alpha^{-1}\chi \\ & = & (\delta^{-1}\beta\delta)^{-1} \;=\; \kappa^{-1} & \end{array}$$

hence

$$\lambda\mu'\lambda = \lambda(\kappa\mu\kappa)\lambda = (\kappa^{-1}\kappa)\mu(\kappa\kappa^{-1}) = \mu.$$

What this means is that the procedure works: Bob can send messages to Alice, and Alice can decode them. Moreover, this procedure is much faster than RSA (by a factor of 20 for realistic values of n), and speed is extremely important in cryptography.

Unfortunately, however, this cryptosystem is not secure.

7.3 Primality Tests

Fermat's Little Theorem says that if p is a prime and a an integer not divisible by p, then $a^{p-1} \equiv 1 \bmod p$. This can be turned into a primality test:

```
1.  Pick some random integer 0 < a < n;
2.  Check whether d := gcd(a,n) = 1;
     if not, print ``d is a factor of n'' and terminate;
```

```
3.  Check whether a^{p-1} ≡ 1 mod p;
      if not, print ``n is composite''.
```

Any integer n surviving this test is called a pseudoprime to basis a; as the example $a = 2$, $n = 341$ shows, there exist composite pseudoprimes.

The primality test given above can be turned into an algorithm that *proves* n to be a prime if it is one; here's the idea: we know that if n is prime, then $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic, generated by a primitive root g. We know that $p-1$ is the smallest positive exponent k of g such that $g^k \equiv 1 \bmod p$. In particular, $g^{(p-1)/q} \not\equiv 1 \bmod p$ for every prime divisor q of $p-1$. Now we claim

Theorem 7.2. *If n and a are integers such that*

1. *$a^{n-1} \equiv 1 \bmod n$ and*
2. *$a^{(n-1)/q} \not\equiv 1 \bmod n$ for every prime divisor q of $p-1$,*

then n is a prime, and a is a primitive root modulo n.

Proof. Let r be the order of $a \bmod n$. Then r divides $n-1$ by Proposition 6.5. We claim that $r = n-1$. If not, then $n-1 = rs$ with $s > 1$, hence there is a prime factor $q \mid s$, i.e., $s = qt$ and $n-1 = rqt$. Then $a^{(n-1)/q} = a^{rt} = (a^r)^t \equiv 1^t = 1 \bmod n$ contradicting 2, so we conclude that $r = n-1$.

Since $a^{n-1} \equiv 1 \bmod n$, we must have $\gcd(a,n) = 1$ (if we had $q \mid a$ and $q \mid n$, then $q \mid a \Longrightarrow q \mid a^{n-1}$ and $q \mid n \Longrightarrow q \mid a^{n-1} - 1$ (from 1.), and this implies $q \mid 1$: contradiction). Thus the powers of $a \bmod n$ generate $n-1$ different residue classes modulo n, all of them coprime to n. Thus every nonzero residue class mod n has an inverse, hence n is prime (and a is a primitive root mod p): this is because if $n = de$ is a nontrivial factorization, then the residue class $d \bmod n$ is nonzero but does not have an inverse. $\square$

Here's a baby-example: take $n = 127$; then $n - 1 = 126 = 2 \cdot 3^2 \cdot 7$. Let us start with $a = 2$ (why not?). We first check that $2^{126} \equiv 1 \bmod 127$. Next we have to make sure that $2^{126/q} \not\equiv 1 \bmod 127$ for $q = 2, 3$ and 7. But already for $q = 2$ we find $2^{63} \equiv 1 \bmod 127$, and our algorithm fails.

Let's see if we are more successful with $a = 3$; again we find $3^{126} \equiv 1 \bmod 127$; now

$$\begin{aligned} 3^{63} &\equiv -1 \bmod 127, \\ 3^{42} &\equiv -20 \bmod 127, \\ 3^{18} &\equiv 18 \bmod 127, \end{aligned}$$

so 127 is indeed prime.

Thus it seems that with a few additional computations we can turn Fermat's little theorem into an algorithm that allows us to prove that a given integer is prime (or not). The problem, however, is this: in step 2, we need the complete factorization of $n-1$. Sometimes this is not a big problem, especially for numbers of the form $n = 2^k m + 1$ with small m, but for general integers this is indeed the bottleneck.

There are, however, improvements to this simple test: first, it can be shown that it suffices to know the factorization of a large part of $n-1$: the part of $n-1$ that we can factor has to be $> \sqrt{n}$.

The primality test given above works well if the prime factorization of $N-1$ is known. This is the case e.g. for Fermat numbers $N = F_n = 2^{2^n}+1$, where $N-1$ is a power of 2. We find:

Proposition 7.3. *A Fermat number F_n is prime if and only if $3^{(F_n-1)/2} \equiv -1 \bmod F_n$.*

Proof. The proof of the "only if" part will be deferred until we know about quadratic residues. Assume therefore that $3^{(F_n-1)/2} \equiv -1 \bmod F_n$; then Theorem 7.2 is satisfied with $a = 3$. □

7.4 Pollard's $p-1$-Factorization Method

Pollard is definitely the world champion in inventing new methods for factoring integers. One of his earliest contributions were the $p-1$-method (ca. 1974), his ρ-method followed shortly after, and his latest invention is the number field sieve (which is based on ideas from algebraic number theory).

The idea behind Pollard's $p-1$-method is incredibly simple. Assume that we are given an integer N that we want to factor. Fix an integer $a > 1$ and check that $\gcd(a, N) = 1$ (should $d = \gcd(a, N)$ be not trivial, then we have already found a factor d and continue with N replaced by N/d).

Let p be a factor of N; by Fermat's Little Theorem we know that $a^{p-1} \equiv 1 \bmod p$, hence $D := \gcd(a^{p-1}-1, N)$ has the properties $p \mid D$ and $D \mid N$. Thus D is a nontrivial factor of N unless $D = N$ (which should not happen too often).

The procedure above is not much of a factorization algorithm as long as we have to know the prime factor p beforehand. The prime p occurs at two places in the method above: first, as the modulus when computing $a^{p-1} \bmod p$. But this problem is easily taken care of because we may simply compute $a^{p-1} \bmod N$. It is more difficult to get rid of the p in the exponent: the fundamental observation is that we can replace the exponent $p-1$ above by any multiple, and D still will be divisible by p (note though that the chance that $D = N$ has become slightly larger). Does this help us? Not always; assume, however, that $p-1$ is the product of *small* primes (say of primes below a bound B that in practice can be taken to be $B = 10^5$ or $B = 10^6$, depending on the computing power of your hardware). Then it is not too hard to come up with good candidates for multiples of $p-1$: we might simply pick $k = B!$, or, in a similar vein,

$$k = \prod_i p_i^{a_i}, \quad \text{where } p_i^{a_i} \le B < p_i^{a_i+1}. \tag{7.1}$$

If we $(p-1) \mid k$, then $a^k \equiv 1 \bmod p$, hence $p \mid D = \gcd(a^k-1, N)$.

Thus the following algorithm has a good chance of finding those factors p of N for which $p-1$ has only small prime factors:

```
1.  Pick a > 1 and check that gcd(a, N) = 1
2.  Choose a bound B, say B = 10^4, 10^5, 10^6, ...
3.  Pick k as in (7.1) and compute D = gcd(a^k - 1, N).
```

Note that the computation of a^k can be done modulo N; if $p \mid N$ and $(p-1) \mid k$, then $a^k \equiv 1 \bmod p$, hence $p \mid D$.

If $D = 1$, we may increase k; if $D = N$, we can reduce k and repeat the computation.

Among the record factors found by the $p-1$-method is the 37-digit factor $p = 6902861817667290192729108442204980121$ of $71^{77}-1$ with $p-1 = 2^3 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 401 \cdot 409 \cdot 3167 \cdot 83243 \cdot 83983 \cdot 800221 \cdot 2197387$ discovered by Dubner. A list of record factors can be found at
`http://www.users.globalnet.co.uk/~aads/Pminus1.html`

Here's a baby example: take $N = 1769$, $a = 2$ and $B = 6$. Then we compute $k = 2^2 \cdot 3 \cdot 5$ and we find $2^{60} \equiv 306 \bmod 1769$, $\gcd(305, 1769) = 61$ and $N = 29 \cdot 61$. Note that $61 - 1 = 2^2 \cdot 3 \cdot 5$, so the factor 61 was found, while $29 - 1 = 2^2 \cdot 7$ explains why 29 wasn't (although $29 < 61$).

Another large class of factorization algorithms is based on an algorithm invented by Fermat: the idea is to write an integer n as a difference of squares. If $n = x^2 - y^2$, then $n = (x-y)(x+y)$, and unless this is the trivial factorization $n = 1 \cdot n$, we have found a factor.

Another baby example: take $n = 1073$; then $\sqrt{n} = 32.756\ldots$, so we start by trying to write $n = 33^2 - y^2$. Since $33^2 - 1073 = 16$, we find $n = 33^2 - 4^2 = (33-4)(33+4) = 29 \cdot 37$. If the first attempt would have been unsuccessful, we would have tried $n = 34^2 - y^2$, etc.

In modern algorithms (continued fractions, quadratic sieve, number field sieve) the equation $N = x^2 - y^2$ is replaced by a congruence $x^2 \equiv y^2 \bmod N$: if we have such a thing, then $\gcd(x-y, N)$ has a good chance of being a nontrivial factor of N. The first algorithm above constructed such pairs (x, y) by computing the continued fraction expansion of $\sqrt{n}$ (which we have not discussed), the number field sieve produces such pairs by factoring certain elements in algebraic number fields.

Exercises

7.1 ISBN

Chapter 8

Quadratic Residues

Quadratic Reciprocity belongs to the highlights of every introduction to number theory. Conjectured by Euler and partially proved by Legendre in the late 18th century, the first complete proof was published 1801 in Gauss's Disquisitiones Arithmeticae (actually he gave two proofs there, followed later by six others).

8.1 Quadratic Residues

Let F be a field; it is an apparently simple question to ask for a characterization of the squares in F, that is, the set of elements $a \in F$ such that $a = b^2$ for some $b \in F$. This question is trivial for $F = \mathbb{C}$ because every complex number is a square. The answer is also easy for $F = \mathbb{R}$: a real number x is a square if and only if $x \geq 0$.

Knowledge about squares is important for solving quadratic equations: $x^2 + ax + b = 0$ has solutions in the reals if and only if the discriminant $a^2 - 4b$ of the polynomial is a square. The same thing is true for finite fields $\mathbb{Z}/p\mathbb{Z}$ for odd p (the case $p = 2$ is different because the formula for solving quadratic equations has a 2 in the denominator, and $2 = 0$ in $\mathbb{Z}/2\mathbb{Z}$): consider e.g. $x^2+2x-1 = 0$ over $\mathbb{Z}/p\mathbb{Z}$. The well known fomula gives the two solutions $\frac{1}{2}(-2 \pm \sqrt{8}\,) = -1 \pm \sqrt{2}$, so there are exactly two solutions if 2 is a square in $\mathbb{Q}(\sqrt{p}\,)$, and none otherwise.

Example. For $p = 7$, $2 \equiv 3^2 \bmod 7$, so the formula gives the two solutions $-1 \pm 3 \equiv 2, -4 \bmod 7$, and in fact $2^2 + 2 \cdot 2 - 1 \equiv (-4)^2 + 2 \cdot (-4) - 1 \equiv 0 \bmod 7$.

Quadratic reciprocity helps us deciding whether certain elements are squares in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ or not. We will call the squares in $\mathbb{F}_p$ (or, more exactly, the integers whose residue classes in $\mathbb{F}_p$ are squares) *quadratic residues* modulo p, the nonsquares *quadratic nonresidues*. Let us make some experiments; since 0 is always a square, we restrict ourselves to $\mathbb{F}_p^\times$.

prime	squares	nonsquares
3	1	2
5	$1, 4$	$2, 3$
7	$1, 2, 4$	$3, 5, 6$
11	$1, 3, 4, 5, 9$	$2, 6, 7, 8, 10$
13	$1, 3, 4, 9, 10, 12$	$2, 5, 6, 7, 8, 11$

There are hardly any regularities to discover. One may notice that the sums of the squares in $\mathbb{F}_p$ are divisible by p for $p > 3$ (can you prove that?), but we want to get a grip on the elements, not on sums (what about products?) of them.

Clearly 1 is always a square; we have also seen that -1 is a square if and only if $p \equiv 1 \bmod 4$. We will now give a slightly different proof using

Proposition 8.1 (Euler's Criterion). *If $a \in \mathbb{Z}$ is not divisible by p, then a is a quadratic residue or nonresidue modulo p according as $a^{(p-1)/2} \equiv +1$ or $a^{(p-1)/2} \equiv -1 \bmod p$.*

Proof. This is easy: assume that $a \equiv x^2 \bmod p$; then $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \bmod p$ by Fermat's Little Theorem.

Conversely, assume that $a^{(p-1)/2} \equiv +1 \bmod p$ and let g be a primitive root modulo p. Then $a \equiv g^r \bmod p$ for some $0 \le r < p-1$; if r were odd, then $a^{(p-1)/2} \equiv (g^{(p-1)/2})^r \equiv (-1)^r = -1 \bmod p$, hence r must be even, say $r = 2s$. But then $a \equiv (g^s)^2 \bmod p$ is a quadratic residue. □

At this point it is appropriate to introduce the Legendre symbol. Given a prime p and an integer $a \in \mathbb{Z}$ with $p \nmid a$, we put

$$\Big(\frac{a}{p}\Big) = \begin{cases} +1, & \text{if } a^{(p-1)/2} \equiv +1 \bmod p, \\ -1, & \text{if } a^{(p-1)/2} \equiv -1 \bmod p. \end{cases}$$

By Euler's criterion, we have $(\frac{a}{p}) = +1$ if a is a quadratic residue modulo p, and $(\frac{a}{p}) = -1$ if a is a quadratic nonresidue. Observe that we have $a^{(p-1)/2} \equiv (\frac{a}{p}) \bmod p$ whenever a is not divisible by p. If we put $(\frac{a}{p}) = 0$ whenever $p \mid a$, the congruence $a^{(p-1)/2} \equiv (\frac{a}{p}) \bmod p$ holds for all integers a.

Corollary 8.2. *The integer -1 is a quadratic residue modulo an odd prime p if and only if $p \equiv 1 \bmod 4$. In other words: $(\frac{-1}{p}) = (-1)^{(p-1)/2}$.*

Proof. By Euler's criterion, -1 is a quadratic residue modulo p if and only if $(-1)^{(p-1)/2} = +1$ (modulo p, but since p is odd, this implies equality). This in turn holds if and only if the exponent $\frac{p-1}{2}$ is even, that is, if and only if $p \equiv 1 \bmod 4$. □

That's not much, but better than nothing. As a matter of fact, this simple result allows us to prove that there are infinitely many primes of the form $4n-1$. We first formulate a little

Lemma 8.3. *If $p > 0$ is an odd prime divisor of an integer of the form $n^2 + 1$, then $p \equiv 1 \bmod 4$.*

Proof. From $p \mid n^2 + 1$ we deduce that $n^2 \equiv -1 \bmod p$. Thus -1 is a quadratic residue modulo p, hence $p \equiv 1 \bmod 4$. □

Corollary 8.4. *There are infinitely many primes of the form $4n + 1$.*

Proof. Assume there are only finitely many primes of the form $4n + 1$, say $p_1 = 5, p_2, \ldots, p_n$. Then $N = 4p_1^2 \cdots p_n^2 + 1$ is of the form $4n + 1$ and greater than all the primes p_k of this form, hence N must be composite. Now N is odd, hence so is any prime divisor p of N, and since any such p is of the form $4n + 1$ by Corollary 8.2, we conclude that $p = p_k$ for some index k. But then $p_k \mid N$ and $p_k \mid N - 1 = 4p_1^2 \cdots p_n^2$, and we get the contradiction that $p_k \mid (N - (N - 1)) = 1$. □

Now let us study the behaviour of the prime 2:

p	3	5	7	11	13	17	19	23	29	31
$(2/p)$	-1	-1	$+1$	-1	-1	$+1$	-1	$+1$	-1	$+1$
$\sqrt{2}$	$-$	$-$	± 3	$-$	$-$	± 6	$-$	± 5	$-$	± 8

Thus 2 is a quadratic residue modulo 7, 17, 23, and 31; among the primes in this table, these are exactly the primes of the form $p \equiv \pm 1 \bmod 8$. Thus we conjecture:

Proposition 8.5. *The prime 2 is a quadratic residue modulo an odd prime p if and only if $p \equiv \pm 1 \bmod 8$. In other words: we have $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$.*

The fact that the second claim is equivalent to the first is easy to check: Basically, the proof boils down to the following table:

$a \bmod 8$	1	3	5	7
$\frac{1}{8}(a^2 - 1) \bmod 2$	0	1	1	0

Great. Now how would one prove such a conjecture? Euler's criterion does not really seem to help, because we have no idea how to evaluate $2^{\frac{p-1}{2}} \bmod p$.

There is a simple proof that 2 is a quadratic residue modulo primes $p = 8k + 1$: let g be a primitive root modulo p and put $s = g^k + g^{-k}$. Then $s^2 \equiv g^{2k} + g^{-2k} + 2 \bmod p$; but $g^{2k} + g^{-2k} = g^{-2k}(g^{4k} + 1) \equiv 0 \bmod 4$ since $g^{4k} \equiv -1 \bmod p$. Thus $s^2 \equiv 2 \bmod p$.

There's actually a classical idea behind this trick: look at the eighth roots of unity in the complex numbers, say $\zeta = e^{2\pi i/8}$. Then $\sqrt{2} = \zeta + \zeta^{-1}$: in fact, $(\zeta + \zeta^{-1})^2 = i + i^{-1} + 2 = 2$ since $1/i = -i$, and moreover $\zeta + \zeta^{-1} > 1$ on the real line (sketch!). Our proof above was merely a translation of this computation from $\mathbb{C}$ to $\mathbb{Z}/p\mathbb{Z}$.

It is possible to do something similar (even for the general reciprocity law) by constructing $\sqrt{p}$ out of roots of unity; this requires some algebra, however, and we will choose a different proof with an elementary flavor.

For computing $(-3/p)$, the algebra involved is simple enough. We claim

Proposition 8.6. *For primes $p > 3$, we have*

$$\Big(\frac{-3}{p}\Big) = \begin{cases} +1 & \text{if } p \equiv 1 \bmod 3, \\ -1 & \text{if } p \equiv 2 \bmod 3. \end{cases}.$$

Proof. Before we go into details, here's the idea: if $p = 3n + 1$, let g be a primitive root mod p, put $\rho = g^n$, and show that $(\rho^2 - \rho)^2 \equiv -3 \bmod p$.

Conversely, if $x^2 \equiv -3 \bmod p$, put $\rho \equiv (-1 + x)/2 \bmod 3$ and show that ρ has order 3; since the order of ρ divides $p - 1$ by Proposition 6.5, we must have $p \equiv 1 \bmod 3$.

Now let's do it properly. Assume first that $p = 3n+1$. We want to construct a square root of $-3 \bmod p$. To this end, pick a primitive root $g \bmod p$ and put $\rho = g^n \bmod p$. Then $\rho^3 \equiv 1 \bmod p$ by Fermat's Little Theorem, and $\rho \not\equiv 1 \bmod p$ since g is a primitive root. Thus $0 \equiv \rho^3 - 1 = (\rho - 1)(\rho^2 + \rho + 1) \bmod p$, and since $p \nmid (\rho - 1)$, we conclude that $\rho^2 + \rho + 1 \equiv 0 \bmod p$. But then $(\rho^2 - \rho)^2 = \rho^4 - 2\rho^3 + \rho^2 \equiv \rho - 2 + \rho^2 \equiv 1 + \rho + \rho^2 - 3 \equiv -3 \bmod p$, and we have shown that -3 is a square modulo p.

Now assume conversely that $x^2 \equiv -3 \bmod p$. We put $\rho \equiv \frac12(-1 + x) \bmod p$, where $\frac12 \bmod p$ denotes the inverse of $2 \bmod p$, and find that $\rho^2 \equiv \frac14(1 - 2x + x^2) \equiv \frac12(-1 - x) \bmod p$ since $x^2 \equiv -3 \bmod p$. But then $\rho^3 \equiv \frac14(1 - x^2) \equiv 1 \bmod p$, so the order of $\rho \bmod p$ divides 3. We claim that the order is 3; if not, the order would have to be 1, and this implies $\rho \equiv 1 \bmod p$; but $p \mid (\rho - 1) = \frac12(-3 + x)$ implies $x \equiv 3 \bmod p$, hence $x^2 \equiv 9 \bmod p$ contradicting $x^2 \equiv -3 \bmod p$ whenever $p \neq 3$. □

8.2 Gauss's Lemma

The main ingredient of the elementary proofs of the quadratic reciprocity law is a lemma that Gauss invented for his third proof. Recall how we proved Fermat's Little Theorem: we took a complete set of prime residue classes $\{1, 2, \ldots, p - 1\}$, multiplied everything by a, and pulled out the factor a^{p-1}. For quadratic reciprocity, Euler's criterion suggests that we would like to pull out a factor $a^{(p-1)/2}$. That's what made Gauss introduce a halfsystem modulo p: this is any set $A = \{a_1, \ldots, a_m\}$ of representatives for residue classes modulo $p = 2m + 1$ with the following properties:

a) the a_j are distinct modulo p, that is: if $a_i \equiv a_j \bmod p$, then $i = j$;

b) every integer is either congruent modulo p to a_i or to $-a_i$ for some $1 \le i \le \frac{p-1}{2}$.

In other words: a halfsystem A is any set of integers such $A \cup -A$ is a complete set of prime residue classes modulo p. A typical halfsystem modulo p is the set $A = \{1, 2, \ldots, \frac{p-1}{2}\}$.

Now consider the prime $p = 13$, choose $A = \{1, 2, 3, 4, 5, 6\}$, and look at $a = 2$. Proceeding as in the proof of Fermat's Little Theorem, we multiply everything in sight by 2 and find

$$\begin{aligned}
2 \cdot 1 &\equiv +2 \bmod 13, \\
2 \cdot 2 &\equiv +4 \bmod 13, \\
2 \cdot 3 &\equiv +6 \bmod 13, \\
2 \cdot 4 &\equiv -5 \bmod 13, \\
2 \cdot 5 &\equiv -3 \bmod 13, \\
2 \cdot 6 &\equiv -1 \bmod 13.
\end{aligned}$$

Thus three products still lie in A, while three others lie in $-A$. Thus there is an odd number of sign changes, and 2 is a quadratic nonresidue.

What about $a = 3$? Here we find

$$\begin{aligned}
3 \cdot 1 &\equiv +3 \bmod 13, \\
3 \cdot 2 &\equiv +6 \bmod 13, \\
3 \cdot 3 &\equiv -4 \bmod 13, \\
3 \cdot 4 &\equiv -1 \bmod 13, \\
3 \cdot 5 &\equiv +2 \bmod 13, \\
3 \cdot 6 &\equiv +5 \bmod 13.
\end{aligned}$$

Here the number of sign changes is even (there are two), and 3 is a quadratic residue modulo 13.

Gauss realized that this is not an accident:

Lemma 8.7 (Gauss's Lemma). *Let $p = 2n + 1$ be an odd prime, put $A = \{a_1, \dots, a_n\}$, and let a be an integer not divisible by p. Write*

$$a_i a \equiv (-1)^{s(i)} a_{t(i)} \bmod p \tag{8.1}$$

for every $a_i \in A$, where $s(i) \in \{0, 1\}$ and $t(i) \in \{1, 2, \dots, n\}$. Then

$$a^n \equiv \prod_{i=1}^{n} (-1)^{s(i)} \bmod p.$$

Thus a is a quadratic residue or nonresidue modulo p according as the number of sign changes is even or odd. The proof is quite simple:

Proof. Observe that the $a_{t(i)}$ in (8.1) run through A if the a_i do, that is: the $a_{t(i)}$ are just the a_i in a different order. In fact, if we had $a_i a \equiv (-1)^{s(i)} a_{t(i)} \bmod p$ and $a_k a \equiv (-1)^{s(k)} a_{t(k)} \bmod p$ with $a_{t(i)} = a_{t(k)}$, then dividing the first congruence by the second gives $a_{t(i)}/a_{t(k)} \equiv (-1)^{s(i)-s(k)} \bmod p$, that is, we have $a_{t(i)} \equiv \pm a_{t(k)} \bmod p$ for some choice of sign. But this is impossible since $1 \le a_{t(i)}, a_{t(k)} \le \frac{p-1}{2}$.

Now we apply the usual trick: if two sets of integers coincide, then the product over all elements must be the same. In our case, this means that $\prod_{i=1}^n a_i a \equiv \prod_{i=1}^n (-1)^{s(i)} a_{t(i)} \bmod p$. The left hand side equals $(a_1 a) \cdot (a_2 a) \cdots (a_n a) = a^n \prod_{i=1}^n a_i$, whereas the right hand side is $\prod_{i=1}^n (-1)^{s(i)} \cdot \prod_{i=1}^n a_{t(i)}$. But we have $\prod_{i=1}^n a_{t(i)} = \prod_{i=1}^n a_i$ by the preceding paragraph. Thus we find $a^n \prod_{i=1}^n a_i \equiv \prod_{i=1}^n (-1)^{s(i)} \prod_{i=1}^n a_i$, and since the product over the a_i is coprime to p, it may be canceled; this proves the claim. $\square$

Let's apply this to give a proof for our conjecture that $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$. We have to count the number of sign changes when we multiply the "half system" $A = \{1, 2, \ldots, \frac{p-1}{2}\}$ by 2. Assume first that $p = 4k+1$, i.e. $\frac{p-1}{2} = 2k$.

$$\begin{aligned}
[1] \cdot [2] &= [2] \\
[2] \cdot [2] &= [4] \\
\ldots &= \ldots \\
[k] \cdot [2] &= [2k] \\
[k+1] \cdot [2] &= [2k+2] \;=\; -[2k-1] \\
\ldots &= \ldots \\
[2k] \cdot [2] &= [4k] \;=\; -[1]
\end{aligned}$$

Here $2a \le 2k$ for $a < k$, that is for $a = 1, 2, \ldots, k$, so there are no sign changes at all for these a. If $k < a \le 2k$, however, then $2k < 2a \le p-1$, hence $1 \le p - 2a < p - 2k = 2k+1$, which implies that there are sign changes for each a in this interval. Since there are exactly k such a, Gauss's Lemma says that $(\frac{2}{p}) = (-1)^k$; we only have to check that $k \equiv \frac{p^2-1}{2} \bmod 2$. But this follows from $\frac{p^2-1}{8} = \frac{1}{8}(p-1)(p+1) = \frac{1}{8} \cdot 4k(4k+2) = k(2k+1)$.

Now assume that $p = 4k-1$; then there are no sign changes whenever $1 \le a \le k-1$, and there are exactly k sign changes for $k \le a < 2k$, so again we have $(\frac{2}{p}) = (-1)^k$. But now $\frac{p^2-1}{8} = \frac{1}{8}(p-1)(p+1) = (2k-1)k$ shows that $k \equiv \frac{p^2-1}{2} \bmod 2$, and we have proved

Proposition 8.8. *The prime* 2 *is a quadratic residue of the odd prime* p *if and only if* $p = 8k \pm 1$*; in other words:* $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$.

As a corollary, consider the Mersenne numbers M_q, where q is odd and $p = 2q+1$ is prime. If $q \equiv 3 \bmod 4$, then $p \equiv 7 \bmod 8$, hence $(2/p) = 1$. By Euler's criterion, this means that $2^q = 2^{(p-1)/2} \equiv 1 \bmod p$, and this in turn shows that $p \mid M_q$.

Corollary 8.9. *If* $p = 2q+1 \equiv 7 \bmod 8$ *is prime, then* $p \mid M_q$*, the* q*-th Mersenne number.*

In particular, $23 \mid M_{11}$ and $83 \mid M_{41}$. Thus some Mersenne numbers can be seen to be composite without applying the Lucas-Lehmer test. There are similar (but more complicated) rules for $p \mid M_q$ when $p = 4q+1$; in this case, we have to study $2^{(p-1)/4} \bmod p$, which leads us to quartic reciprocity. There is a quartic reciprocity law, but this cannot be formulated in $\mathbb{Z}$: Gauss realized in 1832[1] one has to enlarge $\mathbb{Z}$ to the ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$ to do that.

8.3 The Quadratic Reciprocity Law

Here it comes:

Theorem 8.10. *For distinct odd primes p and q, we have*

$$\Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

What Theorem 8.10 says is that p is a square modulo q if and only if q is a square modulo p, except in the case where both p and q are $\equiv 3 \bmod 4$, when p is a square modulo q if and only if q is a nonsquare modulo p. This is a very surprising result, because at first sight the worlds $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$ seem totally different, and there is no apparent reason why they should be related at all. A preliminary version of the reciprocity law was discovered already around 1742 by Euler in his research on prime divisors of numbers of the form $a^n \pm b^n$ (like Mersenne or Fermat numbers), and Euler's final version was published 1785 (two years after his death). It was rediscovered by Legendre in 1788, who gave an incomplete proof. When the Gauss rediscovered it at the age of 18, it took even him a whole year to find a proof (April 8, 1796); he found a simpler proof ten weeks later, but this proof used the theory of binary quadratic forms. The proof using Gauss's Lemma was his third published proof, and he gave eight different proofs altogether.

The proof we shall give is Eisenstein's version of Gauss's third proof. It uses the following variant of Gauss's Lemma:

Lemma 8.11 (Gauss's Lemma). *Let $p = 2m + 1$ be an odd prime, a an integer not divisible by p, and $A = \{1, 2, \ldots, m\}$ a half-system modulo p. Write*

$$a \cdot i = pq_i + r_i, \quad 1 \le r_i \le p - 1, \tag{8.2}$$

for $1 \le i \le m$. Then $(\frac{a}{p}) = (-1)^r$, where r is the number of residues r_i that are $> \frac{p}{2}$.

Now let's look at $a \cdot i = pq_i + r_i$; we clearly have $pq_i = ai - r_i$ with $0 < r_i < p$, hence $q_i = \lfloor \frac{ai}{p} \rfloor$. If we sum up all the n equations in (8.2), we therefore get

$$a \sum_{i=1}^{m} i = p \sum_{i=1}^{m} \Big\lfloor \frac{ai}{p} \Big\rfloor + \sum_{i=1}^{m} r_i.$$

What can we say about the r_i? We know that exactly r of them are from the interval $[m+1, 2m]$, hence are equal to $p - a_j$ for some a_j, while the other $m - r$

[1] Actually, around 1816; he was a bit slow in publishing results, if he published them at all.

residues are elements from the half system A. Thus $r_i \equiv 1 + a_j \bmod 2$ for r of the equations, and $r_i \equiv a_j \bmod 2$ for the other $n - r$ equations. This implies $r_1 + \ldots + r_m \equiv r + a_1 + \ldots a_m \bmod 2$, and we get

$$\sum_{i=1}^{m} \left\lfloor \frac{ai}{p} \right\rfloor \equiv p \sum_{i=1}^{m} \left\lfloor \frac{ai}{p} \right\rfloor = a \sum_{i=1}^{m} ia_i - \sum_{i=1}^{m} r_i \equiv r \bmod 2$$

assuming that a is odd. Using Gauss's Lemma, we deduce

Proposition 8.12. *For odd integers a and odd primes $p = 2m + 1$ with $p \nmid a$ we have*

$$\left(\frac{a}{p}\right) = (-1)^r, \quad \text{where } r = \sum_{i=1}^{m} \left\lfloor \frac{ai}{p} \right\rfloor.$$

In particular, if $q = 2n + 1$ is a prime different from p, then we have

$$\begin{aligned} \left(\frac{q}{p}\right) &= (-1)^r, \quad \text{where } r = \sum_{i=1}^{m} \left\lfloor \frac{qi}{p} \right\rfloor, \\ \left(\frac{p}{q}\right) &= (-1)^s, \quad \text{where } s = \sum_{i=1}^{n} \left\lfloor \frac{pi}{q} \right\rfloor \end{aligned}$$

The quadratic reciprocity theorem therefore boils down to the statement that

$$\sum_{i=1}^{m} \left\lfloor \frac{qi}{p} \right\rfloor + \sum_{i=1}^{n} \left\lfloor \frac{pi}{q} \right\rfloor \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \bmod 2.$$

But this follows immediately from Eisenstein's observation that

$$\sum_{i=1}^{m} \left\lfloor \frac{qi}{p} \right\rfloor + \sum_{i=1}^{n} \left\lfloor \frac{pi}{q} \right\rfloor$$

is the number of lattice points inside the rectangle R with corners $(1, 1)$ and $(\frac{p-1}{2}, \frac{q-1}{2})$.

In fact, consider the line L through the origin and (p, q), that is, with the equation $y = \frac{q}{p}x$. There is no lattice point (a point with integral coordinates) on L between $x = 0$ and $x = p$: in fact, if (r, s) were such a point, then $s = \frac{q}{p}r$, that is, $\frac{s}{r} = \frac{q}{p}$ with $0 < r < p$. But the fraction $\frac{q}{p}$ is in its lowest terms since p and q are different primes. The number of lattice points inside the rectangle R with x-coordinate $x = i$ are $(i, 1)$, $(i, 2)$, ..., $(i, \lfloor \frac{qi}{p} \rfloor)$. This means that

$$\sum_{i=1}^{m} \left\lfloor \frac{qi}{p} \right\rfloor$$

is the number of lattice points inside R below L. By the same reasoning (as can be seen by switching the x- and y-axis),

$$\sum_{i=1}^{n} \left\lfloor \frac{pi}{q} \right\rfloor$$

is the number of lattice points inside R and above the line L.

Now let us finish the proof of Proposition 7.3 that the Fermat number F_n is prime if and only if $3^{(F_n-1)/2} \equiv -1 \bmod F_n$. We have to do the "only if" part, so assume that F_n is prime. Then $(3/F_n) = (F_n/3)$, and since $F_n = 2^{2^n} + 1 \equiv 2 \bmod 3$, we find $(3/F_n) = -1$. Euler's criterion now proves the claim.

8.4 The Jacobi Symbol

The reciprocity law for the Legendre symbol is an amazing piece of insight; for computing Legendre symbols, it is less suited. The reason is simple: before we can invert a symbol (n/p), we have to find the prime factorization of n. Here's an example: suppose you want to compute $(39/59)$; then $39 = 3 \cdot 13$, so $(39/59) = (3/59)(13/59) = -(59/3)(59/13)$ bye the quadratic reciprocity law, hence $(39/59) = -(2/3)(7/13) = (7/13)$ by the second supplementary law, so $(39/59) = (13/7) = (-1/7) = -1$.

Now we know that finding the prime factorization of an integer n isn't much fun if n is big. Fortunately, there's a better way: the reciprocity law for the Jacobi symbol. The trick is simple: invert the Legendre symbols as if the composites that occur were primes. In our example, $(39/59) = -(59/39) = -(20/39) = -(5/39) = -(39/5) = -1$.

Why does this work? Well, for a start we have do define what a symbol like $(59/39)$ should mean. This is easy: assume that n is an odd positive integer with prime factorization $= p_1 \cdots p_r$; then we put $(m/n) := (m/p_1) \cdots (m/p_r)$, where the symbols on the right hand side are Legendre symbols; (m/n) is called the Jacobi symbol. Now we claim

Theorem 8.13 (Reciprocity Law for Jacobi Symbols). *If m and n are coprime positive odd integers, then*

$$\Big(\frac{m}{n}\Big)\Big(\frac{n}{m}\Big) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Moreover, we have the supplementary laws

$$\Big(\frac{-1}{n}\Big) = (-1)^{\frac{n-1}{2}}, \quad \Big(\frac{2}{n}\Big) = (-1)^{\frac{n^2-1}{8}}.$$

Thus the quadratic reciprocity law holds for Jacobi symbols! There are two possible approaches to a proof: either we redo our proof of the reciprocity law for the Legendre symbols (the only problem is generalizing Gauss's Lemma to composite values of m), or we reduce the reciprocity law for Jacobi symbols to the reciprocity law for Legendre symbols. We will do the latter here.

Proof. Let us start with the first supplementary law. Write $n = p_1 \cdots p_r$; then

$$\Big(\frac{-1}{n}\Big) = \Big(\frac{-1}{p_1}\Big) \cdots \Big(\frac{-1}{p_r}\Big) = (-1)^{\frac{p_1-1}{2}+\ldots+\frac{p_r-1}{2}}.$$

Thus it remains to show that

$$\frac{n-1}{2} \equiv \frac{p_1-1}{2} + \ldots + \frac{p_r-1}{2} \bmod 2. \tag{8.3}$$

This is done by induction. We start with the observation that $(a-1)(b-1) \equiv 0 \bmod 4$ for odd integers a, b, hence $ab-1 \equiv (a-1)+(b-1) \bmod 4$, and dividing by 2 gives

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \bmod 2.$$

Now use induction.

Now let us treat the reciprocity law similarly. Write $m = p_1 \cdots p_r$ and $n = q_1 \cdots q_s$; then

$$\Big(\frac{m}{n}\Big)\Big(\frac{n}{m}\Big) = \prod_{i=1}^{r}\prod_{j=1}^{s}\Big(\frac{p_i}{q_j}\Big)\Big(\frac{q_j}{p_i}\Big) = \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{(p_i-1)(q_j-1)/4},$$

and our claim will follow if we can prove that

$$\frac{m-1}{2}\frac{n-1}{2} \equiv \sum_{i=1}^{r}\sum_{j=1}^{s}\frac{p_i-1}{2}\frac{q_j-1}{2} \bmod 4.$$

But this follows by multiplying the two congruences you get by applying (8.3) to m and n.

Finally, consider the second supplementary law. Similar to the above, everything boils down to showing

$$\frac{n^2-1}{8} \equiv \frac{p_1^2-1}{8} + \ldots + \frac{p_r^2-1}{8} \bmod 2.$$

Now clearly $16 \mid (a^2-1)(b^2-1)$ (as a matter of fact, even this product is even divisible by 64), hence

$$(ab)^2 - 1 \equiv a^2 - 1 + b^2 - 1 \bmod 16.$$

Now induction does the rest. □

Exercises

8.1 Use Gauss's Lemma to prove that $(\frac{-2}{p}) = +1$ or -1 according as $p \equiv 1, 3 \bmod 8$ or $p \equiv 5, 7 \bmod 8$.

8.2 Show that there are infinitely many primes $p \equiv 1 \bmod 3$.