ELEMENTARY NUMBER THEORY

HOMEWORK 1

- IMPORTANT NOTE 1: In homework and exams, I want complete sentences!
- IMPORTANT NOTE 2: If you do not do your homework, don't come and complain about your grades at the end of the semester.
- IMPORTANT NOTE 3: There will only be three different final grades for the homework: 10 (regular), 5 (irregular), and 0 (almost no homework). Let me remind you that 10 points are the difference between, say, 70 and 80 points in the end.
- IMPORTANT NOTE 4: The following averages are from last semester's course in algebraic number theory:
  - Final average of students who turned in homework regularly: 65
  - Final average of students who turned in homework irregularly: 42
  - Final average of students who did not turn in homework: 27
- IMPORTANT NOTE 5: Same as 2.

(1) Find an example of nonunique factorization in the monoid

$$M = \{1, 6, 11, 16, \ldots\}$$

of numbers of the form $5n + 1$.

Let me start with a nonexample: the factorizations $1936 = 176 \cdot 11 = 121 \cdot 16$ are not witnesses for nonunique factorization because the factors $176 = 11 \cdot 16$ and $121 = 11 \cdot 11$ are not irreducible. In fact, 1936 has a unique factorization into irreducibles: $1936 = 11^2 \cdot 16$.

In fact, such examples can also be found in $\mathbb{Z}$, where $12 = 2 \cdot 6 = 3 \cdot 4$. The point is that both factorizations involve composite integers, and there is only one factorization into irreducibles, namely $12 = 2 \cdot 2 \cdot 3$.

Examples of nonunique factorization are the following:

(a) $6 \cdot 56 = 16 \cdot 21$: these factorizations cannot be refined because all the factors are irreducible in M. In fact, the possible factorizations $6 = 2 \cdot 3$, $56 = 7 \cdot 8 = 14 \cdot 4 = 28 \cdot 2$, $16 = 2 \cdot 8 = 4 \cdot 4$ and $21 = 3 \cdot 7$ are all impossible in M.

(b) If we replace the prime 7 in the example above by 17 (or, more generally, any prime with last digit 7), we get $6 \cdot 136 = 16 \cdot 51$.

(c) $36 \cdot 56 = 21 \cdot 96$ is an example, but not in this form: $36 = 6 \cdot 6$ is reducible, as is $96 = 6 \cdot 16$. Thus we find $6 \cdot 6 \cdot 56 = 21 \cdot 6 \cdot 16$, and cancelling the factor 6 we find the example above.

(d) $21 \cdot 46 = 6 \cdot 161$ are different factorizations into irreducibles.

(e) $16 \cdot 81 = 6 \cdot 6 \cdot 6 \cdot 6$: here the factors are again irreducible, as a simple calculation shows.

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

(a) using induction on n:

The statement is true for $n = 1$. Assume it holds for n; then $(n+2)^2 - 1 = n^2 - 1 + 4n + 4 = n^2 + 4(n+1)$. Since n is odd, $n+1$ is even, and then $4(n+1)$ is divisible by 8. Now the induction assumption implies that $8 \mid (n+2)^2 - 1$.

(b) by computing $n^2 \bmod 8$ for all four "odd" residue classes modulo 8:

If n is odd, then $n \equiv 1, 3, 5, 7 \bmod 8$. This implies $n^2 \equiv 1, 9, 25, 49 \bmod 8$, and reduction modulo 8 shows $n^2 \equiv 1 \bmod 8$.
A word on notation: you may write $3^2 \equiv 1 \bmod 8$, or $[3]^2 = [1]$, or $\overline{3}^2 = \overline{1}$: use a congruence sign for congruences, and an equality sign if you deal with classes.

(c) by looking at the factorizations $8 = 2 \cdot 4$ and $n^2 - 1 = (n-1)(n+1)$:

Since n is odd, we have $n \equiv 1 \bmod 4$ or $n \equiv 3 \bmod 4$. In the first case, $4 \mid n - 1$ and $2 \mid n + 1$, in the second case $2 \mid n - 1$ and $4 \mid n + 1$. In both cases, the product $(n-1)(n+1)$ is divisible by 8.

(3) Factor integers of the form $4n^2 + 1$ for small values of n. List the prime factors that occur and find a rule that describes them.

Here's a short `pari` program that computes these factorizations:

```
for(n=1,10,print(factor(4*n^2+1)))
```

It finds the primes 5, 13, 17, 29, 37 and a few larger ones, whereas 3, 7, 11, 19 are missing. The correct conjecture is that primes dividing $4n^2 + 1$ have the form $p \equiv 1 \bmod 4$. We will prove this conjecture in the next few weeks; actually it will be the most trivial part of the quadratic reciprocity law.

(4) Show that there are infinitely many primes of the form $p \equiv 2 \bmod 3$. (Hint: $N = 3p_1 \cdots p_n + 2$.)

The first few primes $p \equiv 2 \bmod 3$ are $p_1 = 2$, $p_2 = 5$, $p_3 = 11$. Assume that you have found $p_1 \equiv \ldots \equiv p_n \equiv 2 \bmod 3$, and form $N = 3p_1 \cdots p_n - 1$. Then $N \equiv 2 \bmod 3$, and this implies that not all of its prime factors can be $\equiv 1 \bmod 3$ (a product of primes $\equiv 1 \bmod 3$ is always $\equiv 1 \bmod 3$). Thus there exists a prime $p \mid N$ with $p \equiv 2 \bmod 3$. This prime is different from the p_i, because if $p = p_i$, then $p \mid N$ and $p \mid N + 1$, giving the contradiction $p \mid 1$.

Note that the idea $N = 3p_1 \cdots p_n + 2$ will not work: if you start with $p_1 = 2$, you will get $N = 8$, which gives no new prime. Similarly, $p_1 = 2$ and $p_2 = 5$ give $N = 32$. In fact, the proof above will lead to $p \mid 2$, which is not a contradiction because we might have $p = 2$. Here's what you can do: consider only the odd primes $p_i \equiv 2 \bmod 3$; then $N = 3p_1 \cdots p_n + 2$ will be *odd*, and this means that $2 \nmid N$. With this modification, the proof that most of you suggested does actually work.

The same idea shows that there are infinitely many primes of the form $p \equiv 3 \bmod 4$. It fails for primes $p \equiv 1 \bmod 3$ or $p \equiv 1 \bmod 4$, however,

since e.g. an integer $\equiv 1 \bmod 4$ may have only prime factors of the form $p \equiv 3 \bmod 4$.

Dirichlet proved that there are infinitely many primes of the form $p \equiv a \bmod m$ whenever $\gcd(a, m) = 1$. This result is quite deep, and its proof requires analytic techniques.

(5) Take an ISBN from one of your books and verify that it is valid.

There were no problems with this one.