ELEMENTARY NUMBER THEORY

HOMEWORK 4

(1) Select two random primes p, q of about 10 to 20 digits, form $N = pq$, select e coprime to $(p-1)(q-1)$, and send the pair (N, e) to another student in class; similarly, he will send you his pair.

Now exchange messages using RSA. Write down the encrypted messages c you receive, compute an inverse d of e mod $(p-1)(q-1)$ from a Bezout representation, and decode the messages.

You will need pari for this task. For choosing a 11-digit prime, pick a 11-digit random number like 123456789010 (of coourse this is not random - I'm merely illustrating the idea) and then type `p=nextprime(123456789010)` into `pari`. The answer will be $p = 12345678923$. Pick q, and try a few random values e (they need to be odd – why?) coprime to $(p-1)(q-1)$; you can check this by typing in `gcd(e,(p-1)*(q-1))`.

After you've sent off (N, e), compute a Bezout representation with

`bezout(e,(p-1)*(q-1));`

to understand the output, type in `?bezout`. Make sure that d is positive; if not, replace it by $d + (p-1)(q-1)$.

Finally, computing powers modulo N is done via

```
c = Mod(m,N)^e
```

If you type in

```
c = Mod(m^e,N)
```

instead, you will get the same result or an error message, depending on the size of e. Can you explain this?

Please hand in your solution either by printing it or by sending it as an email; do not copy the numbers by hand from pari.

If you start pari and do a calculation, you can copy the content of the window into a text file or an email by right-clicking the blue frame at the top and then choosing edit and mark. Then use the arrow and left-clicks to highlight the portion you want to copy, and press enter. Then copy the content to your files. It also works backwards, i.e., you can copy things from a text file into the pari window.

(2) (From the first round of the German mathematical olympiad 2006; it is the traditionally "easy" first problem).

Find two consecutive integers with the property that the sum of their digits is each divisible by 2006.

Let $\mathrm{sum}(N)$ denote the sum of the digits of an integer written in decimal notation. It is easy to see that if exactly the last m digits of N are nines, then

$$\mathrm{sum}(N+1) = \mathrm{sum}(N) + 1 - 9m$$

(If, for example, the last digit is not a 9, then $\mathrm{sum}(N) = sm(N) + 1$).

Thus if $\mathrm{sum}(N+1) \equiv \mathrm{sum}(N) \bmod 9$, then we must have $\mathrm{sum}(N) \equiv 0 \bmod 2006$ and $1 - 9m \equiv 0 \bmod 2006$. Solving this congruence means finding a Bezout representation of $\gcd(2006, 9) = 1$, but here we can simply write down $1 = 9 \cdot 223 - 2006$. Thus our N should have a tail of 223 nines. Since the sum of digits of N must be divisible by 2006, all we have to do is write 2005 ones (or e.g. 222 nines and a 7 in some order) in front of the 223 nines.

(3) Consider the password $P = 768462011$, and consider the moduli $n_1 = 919$, $n_2 = 929$, $n_3 = 937$, $n_4 = 941$, and $n_5 = 947$ (these are all primes $> \sqrt[3]{P}$).
   (a) Compute $p_i \equiv P \bmod n_i$ with $0 < p_i < n_i$ for $i = 1, \ldots, 5$.
   (b) Solve the system $x \equiv p_i \bmod n_i$ for $i = 1, 2, 3$ using the Chinese remainder theorem (find the Bezout presentations and follow the notes; first solve the first two congruences, then combine it with the third) and check that the smallest positive solution is $x = P$ (feel free to use pari – this is what it's good for).
   (c) Do the same for the system $x \equiv p_i \bmod n_i$ for $i = 2, 3, 5$.

We easily get

$$\begin{aligned} n_1 &\equiv 644 \bmod 919, \\ n_2 &\equiv 643 \bmod 929, \\ n_3 &\equiv 201 \bmod 937, \\ n_4 &\equiv 7 \bmod 941, \\ n_5 &\equiv 868 \bmod 947. \end{aligned}$$

Now let us solve the system of the first three congruences. We start with the first two and compute a Bezout representation for $\gcd(919, 929)$. We get $1 = 929 \cdot 92 - 919 \cdot 93$. By the Chinese Remainder Theorem, we have to put $m_1 \equiv 644 \cdot 929 \cdot 92 - 643 \cdot 919 \cdot 93 = 86111 \bmod 919 \cdot 929$. We can check our computations by reducing mod 919 and 929, and we do indeed find $86111 \equiv 644 \bmod 919$ and $86111 \equiv 643 \bmod 929$.

The second step consists in solving the system

$$\begin{aligned} m_1 &\equiv 86111 \bmod 919 \cdot 929, \\ n_3 &\equiv 201 \bmod 937. \end{aligned}$$

To this end we need a Bezout representation of $\gcd(919 \cdot 929, 937)$, and `pari` tells us that

$$1 = 426 \cdot 919 \cdot 929 - 420953 \cdot 937.$$

Using this result we now put

$$\begin{aligned} m &\equiv 201 \cdot 426 \cdot 919 \cdot 929 - 86111 \cdot 420953 \cdot 937 \\ &\equiv 768462011 \bmod 919 \cdot 929 \cdot 937. \end{aligned}$$

Here's how to do it with `pari`: after typing in

```
x=Mod(644,919)
y=Mod(643,929)
chinese(x,y)
```

`pari` gives the answer `Mod(86111, 853751)`.

Solving the second system with `pari` is now no problem: we find $x \equiv 49880 \bmod 929 \cdot 941$ and $x \equiv 768462011 \bmod 929 \cdot 941 \cdot 947$.

(4) Find all integers with $\phi(m) = 6$.

Since $\phi(p) = p - 1 > 6$ for primes $p > 7$ and $\phi(p) \mid \phi(n)$ whenever $p \mid n$, we see that n is divisible only by primes $p \leq 7$. Thus we may write $n = 2^a 3^b 5^c 7^d$.

If $d > 1$, then $7 \mid \phi(n)$, hence $d \leq 1$. If $c > 0$, then $4 \mid \phi(n)$, hence $c = 0$. If $b > 2$, then $9 \mid \phi(n)$, hence $b \leq 2$. If $a > 2$, then $4 \mid \phi(n)$, hence $a \leq 2$.

Thus we only have to check the numbers $2^a 3^b 7^d$ with $a, b \leq 2$ and $d \leq 1$. We easily find that $\phi(m) = 6$ if and only if $m = 7, 9, 14, 18$.

(5) Show that if g is a primitive root modulo m, then g is a primitive root modulo any n with $n \mid m$.

The first proof is an adaption of the standard proof from abstract algebra that homomorphic images of cyclic groups are cyclic: Consider a residue class $a \bmod n$. Then $a \equiv g^k \bmod m$, hence $a \equiv g^k \bmod n$. Thus every residue class mod n can be written as some power of g, and this implies the claim.

For a proof by hand, I first claim that $\phi(n) \mid \phi(m)$. By induction it is sufficient to prove the claim when $m = np$ for a prime p. Now there are two cases:

(a) $p \nmid n$: then $\phi(m) = (p-1)\phi(n)$.
(b) $p \mid n$: then $\phi(m) = p\phi(n)$.

Now consider the $\phi(m)$ coprime residue classes $1, 2, \ldots, m-1 \bmod m$ (just the first $\phi(m)$ powers of g). If we reduce these modulo n, then exactly k of these residue classes are $\equiv 1 \bmod n$: in fact, just take $1, 1+n, \ldots, 1+(k-1)n$. It is easy to see that there are no others.

On the other hand, the k integers $g^{\phi(n)}, g^{2\phi(n)}, \ldots, g^{k\phi(n)}$ are all $\equiv 1 \bmod n$ and occur in this list: thus these represent exactly the k residue classes $\equiv 1 \bmod n$ among the first $\phi(m)$ powers of g. This implies that none of the integers $g, g^2, \ldots, g^{\phi(n)-1}$ is $\equiv 1 \bmod n$, hence $\mathrm{ord}_n(g) = \phi(n)$, and g is a primitive root modulo n.

(6) (Also from the first round of the German mathematical olympiad 2006): Solve the diophantine equation $x^3 + y^3 = 4(x^2y + xy^2) + 1$. Hint: factor the expression inside the brackets.

Actually I misstated the problem slightly: the equation was $x^3 + y^3 = 4(x^2y + xy^2 + 1)$. The idea of proof is the same, however.

From $(x+y)(x^2 - xy + y^2) = 4xy(x+y) + 1$ we see that $(x+y) \mid 1$, hence $x + y = 1$ or $x + y = -1$.

Assume first that $x + y = 1$, i.e., $y = 1 - x$. Plugging this into the original equation gives $x^2 - x(1-x) + (1-x)^2 = 4x(1-x) + 1$. Subtracting 1 and factoring out $1 - x$ shows

$$-3x(1-x) = 4x(1-x) \qquad \text{or} \qquad 7x(1-x) = 0,$$

leading to $x = 0$ or $x = 1$. Remembering $y = 1 - x$ this gives the two solutions $(0, 1)$ and $(1, 0)$ in this case.

Now assume that $x+y = -1$. As above we get $-(x^2+x(1+x)+(1+x)^2) = 4x(1 + x) + 1$, which leads to $7x^2 + 7x + 2 = 0$. This clearly does not have integer solutions since it is not even solvable mod 7.