

Homework 2

Due Thursday, 10/14/2004

1 Prime Modular Arithmetics

Let p be a prime. Recall groups \mathbb{Z}_p and \mathbb{Z}_p^* from lecture and the handout on modular arithmetics. Recall the fact that \mathbb{Z}_p^* is cyclic and has a generator (in fact it has many of them). Recall set QR_p of squares modulo p .

1.1

Write out the elements of group \mathbb{Z}_{11} . How many elements are there? Pick an element g which is a generator of this group. For every element $a \in \mathbb{Z}_{11}$, write down $DL_{(g,11)}(a)$.

1.2

Let g be a generator of \mathbb{Z}_p^* . Prove that if $g^x = g^y \pmod p$ then $x = y \pmod{p-1}$.

1.3

Let g be a generator of \mathbb{Z}_p^* . Prove that $y \in QR_p$ if and only if $x = DL_{(g,p)}(y)$ is even. (Note that since g is a generator then for every $y \in \mathbb{Z}_p^*$ there is $x = DL_{(g,p)}(y)$.)

Which of the elements of \mathbb{Z}_{11} are squares?

1.4

Prove that $y \in QR_p$ if and only if $y^{(p-1)/2} = 1 \pmod p$.

1.5

Prove that if y, z are quadratic residues modulo p then so is $yz \pmod p$ and $y^{-1} \pmod p$. (In fact this holds for any p , not necessarily prime one.)

1.6

Recall that an *order* $ord_p(a)$ of an element $a \in \mathbb{Z}_p^*$ is defined as the smallest i s.t. $a^i = 1 \pmod p$. The order of the group is the maximum order of any of the group's elements. For each element in \mathbb{Z}_{11} tell its order.

- (1) Can you see a relation between orders of elements of \mathbb{Z}_{11} and number $\phi(11) = 10$?
- (2) Can you formulate a general hypothesis about orders of group elements and $\phi(p)$?
- (3) Can you prove it?

2 Composite Modular Arithmetics

Let $n = pq$ for prime p, q . Recall that by the Chinese Remainder Theorem, for every $r_1 \in \mathbb{Z}_p$ and $r_2 \in \mathbb{Z}_q$ there is a unique $s \in \mathbb{Z}_n$ s.t. $s = r_1 \pmod p$ and $s = r_2 \pmod q$, and vice versa.

2.1

Show how to reconstruct s from (r_1, r_2) if you know elements a, b s.t. $ap + bq = 1$. (Note that $ap = 0 \pmod p$, $ap = 1 \pmod q$, $bq = 0 \pmod q$ and $bq = 1 \pmod p$...)

2.2

Consider group \mathbb{Z}_{35}^* . List its elements. How many of them are there? What's $\phi(35)$?

2.3

Consider the CRT theorem for $n = 35$, $p = 5$, $q = 7$. Find a, b s.t. $ap + bq = 1$ (you can find them by hand or by a Euclidean algorithm). Compute $205^{140} \pmod{35}$ without a computer. Show your work. (Hint: CRT helps here.)

3 Orders of Growth, Polynomial Time

3.1

Explain how you would implement modular multiplication for large moduli p (not necessarily prime). Give the running time of this algorithm assuming that you have a computer that takes $O(1)$ instructions to either *add* two 64-bit numbers or *multiply* two 64-bit numbers (here the output is 128-bit long).

You don't have to be very detailed here! I don't want to get an exact code, and if you do not explain how carry bits are taken care of, that's OK too. All I want is a general idea for this algorithm.

What's the running time of your algorithm? Is it a polynomial-time algorithm?

3.2

Show that if the running time of an algorithm A is $T_A(t) = \Omega(2^t)$ then the algorithm is not polynomial time.

3.3

The time it takes for the best known algorithm A (Number Field Sieve) to factor t -bit long RSA moduli is known to be approximately $T_A(t) = 2^{c(n^{1/3})(\log n)^{2/3}}$ for some constant c and for all t larger than some (small) initial t_0 value.

Show that $T_A(t)$ is *not* polynomial time.

Because of the above running time, the practical hardness of the factoring problem on a random $t = 1024$ bit RSA modulus is believed to be 2^{80} , meaning that the best known algorithm A would take about 2^{80} steps to factor. Knowing this, approximate the c constant in the above equation the best you can.