COS 341: Discrete Mathematics

Homework #9 Fall 2006
Number Theory Due: Friday, December 15

Special late policy: Because this homework is due right before break, there will be a special late policy in which the Saturday, Sunday and Monday following the deadline count together as a single late "day." To be clear, this table shows how many "days" late your assignment will be counted if turned in on the following dates:

Calendar date	**Number of late days charged**
Friday, December 15	0
Monday, December 18	1
Tuesday, December 19	2
Wednesday, December 20	3
Thursday, December 21	*Not accepted on or after this date*

For this homework only, if you are out of the Princeton area over break, you may mail or email your assignment to Mohammad. If mailed, your homework is considered submitted on the post mark date, and should be sent to this address: Mohammad Mahmoody Ghidary, Princeton University, Department of Computer Science, 35 Olden Street, Princeton, NJ 08540. (It would be wise to send him email at the same time you mail your assignment so that he can look out for it; also, save a photocopy of your work.) Note that mailing your assignment may delay when it is graded and returned to you.

See instructions on the "assignments" web-page on how and when to turn in homework, and be sure to read the collaboration and late policy for this course. Approximate point values are given in brackets. *Be sure to show your work and justify your answers.*

1. Let p be a prime number.

a. [4] Prove that $a^2 \equiv b^2 \pmod{p}$ if and only if $a \equiv b \pmod{p}$ or $a \equiv -b \pmod{p}$. Use this to show specifically that a is *self-inverse*, meaning that $a^2 \equiv 1 \pmod{p}$, if and only if $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

b. [7] Wilson's Theorem asserts that if p is a prime, then

$$(p-1)! \equiv -1 \pmod{p}.$$

The English mathematician Edward Waring said that this theorem would probably be very difficult to prove because there was no adequate notation for primes. Gauss proved it while standing (on one foot, it is rumored). He suggested that Waring failed for lack of notions, not notations. Prove Wilson's Theorem. Hint: While standing on one foot, think about pairing each term in $(p-1)!$ with its multiplicative inverse.

2. In this problem, we prove an important and useful result called the *Chinese remainder theorem*. Throughout this problem, assume that m and n are relatively prime.

a. [4] Prove that $mn|c$ if and only if $m|c$ and $n|c$. Use this to show that $s \equiv t \pmod{mn}$ if and only if $s \equiv t \pmod{m}$ and $s \equiv t \pmod{n}$.

b. [5] Prove that for any a, b, there exists a number x such that

$$x \equiv a \pmod{m} \tag{1}$$

and

$$x \equiv b \pmod{n}. \tag{2}$$

Hint: Congruence (1) holds if and only if $x = jm + a$ for some j. So there is such an x only if

$$jm + a \equiv b \pmod{n}.$$

Solve this last congruence for j.

c. [3] Prove that there exists an x satisfying the congruences (1) and (2) such that $0 \leq x < mn$.

d. [4] Prove that the x satisfying part (c) is unique.

3. Let $\phi(n)$ be the number of integers between 1 and $n-1$ which are relatively prime to n. For instance, $\phi(10) = 4$ since $1, 3, 7, 9$ are relatively prime to 10, but $2, 4, 5, 6, 8$ are not.

a. [5] Prove that if p is prime and k is a positive integer, then

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

b. [7] Use the results in the preceding problems to prove that if m and n are positive with $\gcd(m, n) = 1$ then

$$\phi(mn) = \phi(m)\phi(n).$$

4. In class, we studied the RSA cryptosystem. However, we did not give any evidence that it is hard to break RSA other than "proof by reference to eminent authority," i.e., Rivest, Shamir and Adleman as well as a lot of other very smart people over the last few decades were not able to break it.

Here we describe the Rabin public-key cryptosystem, that has slightly better security justification than RSA. That is, if someone has the ability to break this cryptosystem efficiently, then one also has the ability to factor numbers that are products of two primes. Why should that convince us that it is hard to break the cryptosystem efficiently? Well, mathematicians have been trying to factor efficiently for centuries, and they still haven't figured out how to do it. So, we are again appealing to a proof by eminent authority, but at least there are more authorities involved here.

In the Rabin cryptosystem, before any messages are sent, Bob chooses two large prime numbers p and q which must have the property that $p \equiv q \equiv 3 \pmod{4}$. Let $n = pq$. This number n is the public key for the system which is published widely. However, the numbers p and q are kept secret by Bob.

When Alice wants to send Bob a message, she first converts it to a number $m \in \{1, \ldots, n-1\}$, and then computes $c = \text{rem}(m^2, n)$. That is, she simply squares m and takes its remainder modulo n. This number c is her encrypted message, which she sends (over a public wire or network) to Bob.

Later, we will show that Eve, who is eavesdropping on the line, cannot reconstruct m unless she is able to factor n. First, however, we will look at how Bob can reconstruct

Alice's message m with his secret knowledge of p and q. In fact, we will only show how Bob can find four candidate messages, one of which is the actual message m. We will not discuss how to determine which of the four was the actual message, although in practice, the true message can be marked in some way to distinguish it from the others.

Throughout this problem, you should freely make use of results proved elsewhere on this problem set.

a. [1] Show that $(p+1)/4$ and $(q+1)/4$ are integers.

b. [4] Let $s = \text{rem}(c^{(p+1)/4}, p)$ and let $t = \text{rem}(c^{(q+1)/4}, q)$. Prove that

$$s^2 \equiv m^2 \pmod p$$

and

$$t^2 \equiv m^2 \pmod q.$$

c. [3] Show that there exist uniquely determined numbers r_1, r_2, r_3, r_4 between 0 and $n-1$ such that

$$\begin{aligned} r_1 &\equiv s \pmod p & \qquad r_3 &\equiv -s \pmod p \\ r_1 &\equiv t \pmod q & \qquad r_3 &\equiv t \pmod q \end{aligned}$$

$$\begin{aligned} r_2 &\equiv s \pmod p & \qquad r_4 &\equiv -s \pmod p \\ r_2 &\equiv -t \pmod q & \qquad r_4 &\equiv -t \pmod q. \end{aligned}$$

Also show that $r_3 \equiv -r_2 \pmod n$ and that $r_4 \equiv -r_1 \pmod n$.

d. [5] Prove that the original message m is equal to one of the four numbers r_1, r_2, r_3, r_4. Thus, knowing p and q, Bob can compute s and t, and can then find r_1, r_2, r_3, r_4 (this can be done efficiently), one of which must be the original message m.

e. [6] Next, we show that if Eve has an algorithm for breaking this cryptosystem, then she can use it to factor n. The argument above shows that the congruence

$$x^2 \equiv c \pmod n$$

has only the four solutions, r_1, r_2, r_3, r_4. Suppose that Eve, without knowledge of p and q, is somehow, on some message c, able to compute this same set of four numbers. Prove that with knowledge of n, c and the four numbers (but not p, q, s or t), Eve can efficiently determine p and q.