MATH 3320, HOMEWORK #6

DUE FRIDAY, OCTOBER 5

To ensure that you get full credit, be sure to *show your work* in the problems that require calculations. Very little credit is given for answers without justification. Please write in complete sentences to help us understand what you are doing.

You may collaborate with classmates in solving the problems, including the extra credit problems. If you do so, please list their names on your assignment. However, you should not consult *any* other people (except the instructors or TAs), or use online resources. (Seriously, it's very obvious to us when this occurs, and there are drastic consequences, so don't do it!) If you use results that were not proved in class, please provide your own proof.

1. (15 points) Let p be a prime number and take any positive divisor e of $p-1$. Prove that there is an $a \in \mathbf{Z}$ that is relatively prime to p and that has order e modulo p.

2. Bob wants to be able to receive messages from Alice using RSA. He picks primes $p = 19$ and $q = 23$ and $e = 7$. (Confirm for yourself that e is a valid choice of exponent.) Bob publishes $(N, e) = (437, 7)$ as his public key.

(a) (5 points) How can you find Bob's private key k using the Euclidean algorithm?

(b) (10 points) Alice wants to send the message $m = 42$ (note that $0 < m < N$) to Bob. What is the encrypted message that Alice transmits to Bob?

(c) (10 points) Suppose that Bob receives the ciphertext $c = 221$ from Alice. What was the original message m that Alice sent?

3. (Cyclotomic polynomials) Fix an integer $n > 0$, and let $g := e^{\frac{2i\pi}{n}}$. It has order n; i.e. $g^n = 1$, and no smaller power equals 1. The numbers $g^k := e^{\frac{2i\pi k}{n}}$ for $k = 0, \ldots, n-1$ are all the (complex) roots of the equation $X^n - 1 = 0$. So

$$X^n - 1 = \prod_{\zeta^n=1} (X - \zeta) = \prod_{0 \le k \le n-1} (X - g^k).$$

The element g^k has order $n/\gcd(n,k)$. The cyclotomic polynomial $\Phi_n(x)$ is defined as

$$\Phi_n(X) := \prod_{order(\zeta)=n} (X - \zeta) = \prod_{(k,n)=1} (X - g^k).$$

(a) (5 points) Show that the degree of $\Phi_n(X)$ is $\phi(n)$.

(b) (10 points) Show that if p is prime, then $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$.

(c) (10 points) Show that $\Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}})$.

4. (Miller–Rabin Test)

> **Theorem.** Let n be an odd integer. Write $n - 1 = 2^k q$ with q odd. If there is an integer $a < n$ such that
>
> (a) $a^q \not\equiv 1 \ (mod\ n)$
>
> (b) $a^{2^i q} \not\equiv -1 \ (mod\ n)$ for all $0 \le i \le k-1$,
>
> then n is composite.

It is known that for any composite number n, more that 75% of the a $(mod\ n)$ satisfy the test.

(a) (5 points) Use the Miller-Rabin test to show that 3599 and 427 are composite.
(b) (10 points) The Miller-Rabin Primality Test comprises a number of successive squarings. Suppose a 300-digit number n is given. How many squarings are needed in the worst case during a single run of this primality test?

5. (Extra credit) Here is a cryptosystem, apparently proposed at a cryptography conference, that was supposed to be faster than RSA.

There are two parties—Alice and Bob—that want to pass a secret message. Bob wants to send a message to Alice. The procedure goes like this:

- Alice chooses two large primes p and q and takes their product $N = pq$. Then she chooses three random numbers g, r_1, r_2 modulo N and computes
$$g_1 \equiv g^{r_1(p-1)} \pmod N \quad \text{and} \quad g_2 \equiv g^{r_2(q-1)} \pmod N.$$
She transmits her public key (N, g_1, g_2) and keeps her private key (p, q) to herself.
- Bob wants to send the message $m \pmod N$ to Alice. He choose two random numbers $s_1, s_2 \pmod N$, computes
$$c_1 \equiv m g_1^{s_1} \pmod N \quad \text{and } c_2 \equiv m g_2^{s_2} \pmod N,$$
and transmits the ciphertext (c_1, c_2) to Alice.
- Alice solves the pair of congruences
$$x \equiv c_1 \pmod p$$
$$x \equiv c_2 \pmod q$$
using the Chinese Remainder Theorem. (This is certainly *much* faster than RSA.)

(a) (5 points) Show that Alice's solution x is equal to Bob's plaintext m.
(b) (5 points) Explain why this cryptosystem is not secure.

Hints: The primes $\{p, q\}$ satisfy $\alpha p + \beta q = 1$. The two published numbers $\{g_1, g_2\}$ also satisfy $(\alpha p)g_2 + (\beta q)g_1 = 1$ because $g_2 \equiv 1$ $(mod\ q)$ and $g_1 \equiv 1 (mod\ p)$ by Fermat's theorem. The congruence modulo N satisfying $\equiv 1$ $(mod\ p)$ and $\equiv 1$ $(mod\ q)$ (by the Chinese remainder Theorem) is 1, and of the form $(\alpha p)g_2 + (\beta q)g_1$. The same holds for $g_2^{s_2}$ and $g_1^{s_1}$ by the same reasoning; this is useful for part (a).

So
$$\begin{cases} (\alpha p) + (\beta q) = 1 \\ (\alpha p)g_2 + (\beta q)g_1 = 1 \end{cases}$$
From the two equations you can find αp and βq.

The previous part shows that $x = m = c_1(\beta q) + c_2(\alpha p)$; so you have decoded the message.