Math 173A - Presentation Problem Set

1 Basic Number Theory

1. Let $F_1 = 1$, $F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ define the Fibonacci numbers 1, 1, 2, 3, 5, 8, ... Use the Euclidean algorithm to compute $\gcd(F_n, F_{n-1})$ for all $n \geq 1$.

2. Find the last 2 digits of 123^{562}.

3. Here is how to construct the x guaranteed by the general form of the Chinese remainder theorem. Suppose $m_1,\ m_2,\ \ldots,\ m_k$ are integers with $\gcd(m_i, m_j) = 1$ whenever $i \neq j$. Let $a_1,\ a_2,\ \ldots,\ a_k$ be integers. Perform the following procedure.

   (i) For $i = 1, \ldots, k$ and let $z_i = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_k$.

   (ii) For $i = 1, \ldots, k$ and let $y_i \equiv z_i^{-1} \pmod{m}_i$.

   (iii) Let $x = a_1 y_1 z_1 + \cdots + a_k y_k z_k$.

   Show that $x \equiv a_i \pmod{m_i}$ for all i.

4. Let p be an odd prime and let a be an integer that is not divisible by p, and let b be a square root of a modulo p.

   (a) Prove that for some choice of k, the number $b + kp$ is a square root of a modulo p^2.

   (b) Suppose that b i sa square root of a modulo p^n. Prove that for some choice of j, the number $b + jp^n$ is a square root of a modulo p^{n+1}.

   (c) Show that if p is an odd prime and if a has a square root modulo p, then a has a square root modulo p^n for every power of p. Is this true if $p = 2$?

5. Let $n = pq$ with p and q distinct odd primes.

   (a) Suppose that $\gcd(a, pq) = 1$. Prove that if the equation $x^2 \equiv a \pmod{n}$ has any solutions, then it has four solutions.

   (b) Suppose that you had a machine that could find all four solutions for some given n. How could you use this machine to factor n?

6. Let a, b, m, n be integers with $\gcd(m, n) = 1$. Let

$$c \equiv (b - a) \cdot m^{-1} \pmod{n}.$$

   Prove that $x = a + cm$ is a solution to

$$x \equiv a \pmod{m} \qquad \text{and} \qquad x \equiv b \pmod{n}$$

   and that every solution to these simultaneous congruences has the form $x = a + cm + ymn$ for some $y \in \mathbb{Z}$.

2 Euler's ϕ function

1. For any two integers m and n, prove that $\phi(\text{lcm}(m,n)) \cdot \phi(\gcd(m,n)) = \phi(m)\phi(n)$.

2. Let $p_1,\ p_2,\ \ldots,\ p_r$ be the distinct primes that divide N. Prove that

$$\phi(N) = N \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

3. Let N, c, and e be positive integers satisfying the conditions $\gcd(N,c) = 1$ and $\gcd(e, \phi(N)) = 1$. Explain how to solve the congruence

$$x^e \equiv c \pmod{N},$$

assuming you know the value of $\phi(N)$.

4. Find all n such that $\phi(n)$ is odd and prove that you have found all such n.

5. For any positive integer N, prove that

$$\sum_{d|N} \phi(d) = N,$$

where the sum is over all positive divisors of N.

6. For any two integers m and n prove that

$$\phi(mn) = \phi(m)\phi(n) \cdot \frac{\gcd(m,n)}{\phi(\gcd(m,n))}.$$

7. Let M and N be integers satisfying $\gcd(M,N) = 1$. Prove the multiplication formula

$$\phi(MN) = \phi(M)\phi(N).$$

8. Prove that if n has r distinct odd prime factors, then $2r \mid \phi(n)$.

3 Abstract Algebra

1. Show that the set of all invertible 2×2 matrices with entries in $\mathbb{F}_p$ is a noncommutative group for every prime p.

2. Let G be a group and let $d \geq 1$ be an integer. Define a subset of G by

$$G[d] = \{g \in G : g^d = e\}.$$

   (a) Prove that if g is in $G[d]$, then g^{-1} is in $G[d]$.

   (b) Suppose that G is commutative. Prove that if g_1 and g_2 are in $G[d]$, then $g_1 g_2$ is in G as well.

(c) Deduce that if G is commutative, then $G[d]$ is a group.

(d) Show by an example that if G is not a commutative group, then $G[d]$ need not be a group.

3. If $\mathbb{F}$ is a field, we define the *characteristic* of $\mathbb{F}$ to be the smallest positive integer k such that

$$\underbrace{1+1+\cdots+1}_{k \text{ times}} = 0.$$

If there is no such k, we say that $\mathbb{F}$ has characteristic zero.

(a) Give an example of a field with characteristic zero.

(b) Show that if $\mathbb{F}$ is a field with positive characteristic, the characteristic must be a prime number.

4. If m is composite, why is $\mathbb{Z}/m\mathbb{Z}$ not a field?

4 Discrete Logarithms

1. Let p be prime.

(a) Let q be a prime number such that $q \mid p-1$. Prove that $\mathbb{F}_p^\times$ has an element of order q.

(b) Let N be an integer such that $N \mid p-1$. Prove that $\mathbb{F}_p^\times$ has an element of order N.

2. It can be shown that 5 is a primitive root for the prime 1223. You want to solve the discrete logarithm problem $5^x \equiv 3 \pmod{1223}$. Given that $3^{611} \equiv 1 \pmod{1223}$, determine whether x is even or odd.

3. In the Diffie-Hellman key exchange protocol, Alice and Bob choose a primitive root g for a large prime p. Alice sends $x_1 \equiv g^a \pmod{p}$ to Bob and Bob sends $x_2 \equiv g^b \pmod{p}$ to Alice. Suppose Eve bribes Bob to tell her the values of b and x_2. However, Bob forgets to tell Eve the value of g. Suppose $\gcd(b, p-1) = 1$. Show that Eve can determine g from the knowledge of p, x_2 and b.

4. Use the Pohlig-Hellman algorithm to solve the discrete logarithm problem

$$g^x = a$$

in $\mathbb{F}_p$ where $p = 181$, $g = 2$ and $a = 100$.

5. In the ElGamal cryptosystem, Alice and Bob use $p = 17$ and $g = 3$. Alice chooses her secret exponent to be $a = 6$, so $A \equiv 15 \pmod{p}$. Bob sends the ciphertext $(7, 6)$. Find m.

6. Using the baby-step giant-step algorithm, find x so that $5^x \equiv 193 \pmod{503}$. You may use a calculator.

5 RSA

1. Bob uses RSA to receive a single ciphertext c corresponding to the message m. His public modulus is N and his public encryption exponent is e. Since Bob feels guilty that his system was used only once, he agrees to decrypt any ciphertext he receives as long as it's not c, and return the decryption to that person. Eve sends him the ciphertext $2^e c \pmod{N}$. Show how Eve can use this to find m.

2. Suppose you are as system administrator setting up a messaging service for a company. You want users to encrypt their communications using RSA, so you generate public and private keys for them. You do this by generating a list of 100 huge primes, say with 1024 bits each. You then generate each user's public modulus by choosing two primes from this list, being extra careful so that no two users have the same public modulus.

   Explain why if there are more than 50 users on this network, some of the users' communications can be compromised.

3. Alice and Bob are good friends, so they decide to use the same public RSA modulus, but with different encryption exponents e and f. Suppose Charlie encrypts the message m and sends it to Alice and Bob, using their respective public keys in both cases. Show that if Eve can intercept these ciphertexts then she can recover m.

4. Suppose $n = pq$ is a product of two primes and suppose that $\gcd(a, pq) = 1$.

   (a) Show that if $x^2 \equiv a \pmod{n}$ has any solutions in $\mathbb{Z}/n\mathbb{Z}$, then it has exactly four.

   (b) If, for some $a \in \mathbb{Z}/n\mathbb{Z}$, you know all four solutions to $x^2 \equiv a \pmod{n}$, show that you can efficiently factor n.

5. Your opponent uses RSA with $n = pq$ and encryption exponent e and encrypts a message m. This yields the ciphertext $c \equiv m^p \pmod{n}$. A spy tells you that, for this particular message, $m^{12345} \equiv 1 \pmod{n}$. Describe how to determine m.

6 Primality Testing and Factorization

1. (a) What is a Fermat witness for a composite number?

   (b) List all Fermat witnesses for 15.

   (c) What is a Miller-Rabin witness?

   (d) List all Miller-Rabin witnesses for 15.

2. Describe the pollard $p - 1$ algorithm and use it to factor $2^9 - 1$.

3. Recall that a composite number n is a Carmichael number if $a^n \equiv a \pmod{n}$. Show that all Carmichael numbers are odd.

4. Let $N = 561$. Show that $a = 2$ is a Miller-Rabin witness to the compositeness of N and that this can be used to factor N.

5. Suppose m is a positive integer such that $6m + 1$, $12m + 1$ and $18m + 1$ are all primes. Let $n = (6m + 1)(12m + 1)(18m + 1)$. Prove that n is a Carmichael number.