Compilation of Problems

1. Find the greatest common divisor of 1112 and 1544.

2. For the value d of the greatest common divisor found in the first question, find all integer solutions (x, y) to the equation $1112x + 1544y = d$

3. For any positive real number r, prove that $x^r = O(e^x)$ as functions of x.

4. Show that $\sum_{i=1}^n i = O(n^2)$, and $\sum_{i=1}^n i^2 = O(n^3)$ as functions of n.

5. Estimate the number of bit operations needed to add the numbers from 1 to 2^{12} in the most naive manner imaginable.

6. Let p be a prime number and n a positive integer. Show that the largest power of p which divides $n!$ is given by
$$\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor .$$
(Here $\lfloor x \rfloor$ is the largest integer not greater than x).

7. Let p be a prime number. Find all solutions to the congruence $x^2 \equiv 1 \pmod{p}$. Find a positive integer $n \neq 187$ such that $x^2 \equiv 1 \pmod{n}$ has more than two solutions modulo n.

8. Show that 0-13-116093-8 is not a valid ISBN number, and find two diferent valid ISBN numbers that each differ from 0-13-116093-8 in exactly one digit. (This shows that although the ISBN scheme can detect a single error, it cannot correct a single error).

9. Find all solutions of the congruences $12x \equiv 28 \pmod{20}$ and $12y \equiv 30 \pmod{20}$.

10. Find a multiplicative inverse of 7 modulo 30. (ie x such that $7x \equiv 1 \pmod{30}$).

11. If $x \equiv 2 \pmod{7}$ and $x \equiv 3 \pmod{10}$, then what must x be congruent to modulo 70?

12. Find the remainder when 5^{1056} is divided by 7.

13. Find all four solutions to $x^2 \equiv 1 \pmod{187}$.

14. Let p and q be distinct primes. Prove that $\phi(pq) = (p-1)(q-1)$.

15. Prove that the binomial coefficient $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ divides the product
$$\prod_p p^{\lfloor \log_p(2n) \rfloor}$$
where the product is taken over all primes p.

16. Suppose we are in the RSA setup, where N is a product of two disctinct primes, and d and e are two integers with $de \equiv 1 \pmod{\phi(N)}$. Prove that for any integer a (not necessarily relatively prime to N), that $a^{de} \equiv a \pmod{N}$. [This provides a better answer to the question raised in class about what happens when $\gcd(a, N) \neq 1$ (which of course is ridiculously unlikely to happen in practice)].

17. Let N be an integer that is a product of two distinct primes. Show how to quickly factor N if one knows the value of $\phi(N)$.

18. The ciphertext 75 was obtained using the RSA algorithm with $n = 437$ and $e = 3$. You know that the plaintext is a positive integer less than 10. Determine which integer this is without factoring n.

19. Three RSA users have public keys with modulus N_1, N_2, N_3 (you may assume if you want that these moduli are pairwise coprime) and each use the encryption exponent $e = 3$. Suppose that the same message m ($0 \leq m \leq N_i$) is sent to each RSA user, and you intercept the three ciphertexts $c_i \equiv m^3 \pmod{N_i}$ for $i = 1, 2, 3$.

    Show that $0 \leq m^3 \leq N_1N_2N_3$, and hence that using the Chinese remainder theorem, you can not only calculate the value of $m^3 \pmod{N_1N_2N_3}$, but that you actually obtain the exact value of m^3 and hence can read the message m.

20. From Question 9 of the previous problem set, we know the inequality

$$\prod_p p^{\lfloor \log_p(2n) \rfloor} \geq \binom{2n}{n}$$

    where the product is taken over all prime numbers p.

    Using this inequality, prove that there are infinitely many primes. (For this you will need a handle on how large the right hand side is. There is an estimate $\binom{2n}{n} \geq 4^n/(2n+1)$ which is obtained as follows: Expand $4^n = (1+1)^{2n}$ using the binomial expansion. There are a total of $2n + 1$ terms and the largest is $\binom{2n}{n}$. It is also possible to obtain a more precise estimate using Stirling's formula).

21. Let a and n be positive integers with $\gcd(a, n) = 1$. The *order* of a modulo n (denoted $\text{ord}_n(a)$) is defined to be the smallest positive integer d such that $a^d \equiv 1 \pmod{n}$.

    Let r be a positive integer. Prove that $a^r \equiv 1 \pmod{n}$ if and only if r is divisible by $\text{ord}_n(a)$. (This is Exercise 20 in Chapter 3 of Trappe & Washington, which gives out hints for the proof).

22. Compute the continued fraction expansion of the three numbers $427/67$, $\sqrt{7}$ and $\tan(1)$. (For the latter number, you don't need to prove the result you get is correct, simply do enough computations to be able to guess the pattern (and show how these computations were performed). Of course 1 is in radians).

23. Let $n = 8777$. By working out 93^2 and 281^2 modulo n, factor n.

24. At `http://math.stanford.edu/~petermc/math110/pollardrho.gp`, you will see a simple implementation of the Pollard rho factoring algorithm for a simple choice of function $F(x) = x^2 + 1$ with initial value 2. (This program is designed to run in gp/pari). Find a not obviously composite integer n such that running this algorithm fails to factor n. For these purposes, an integer is deemed to be obviously composite if it is divisible by a prime less than 6.

25. Let S be a set with r elements and let $f : S \to S$ be a bijection. Pick $x_0 \in S$ and inductively define $x_{i+1} = f(x_i)$. Let k denote the first index such that there exists $j < k$ with $f(x_k) = f(x_j)$. As F varies over all bijections $S \to S$, prove that the average value of k is $(r+1)/2$.

26. Suppose that the Pollard rho algorithm is implemented with function $F(x) = ax+b$ for some integers a and b. Explain why this is a bad idea.

27. Suppose that the Pollard rho algorithm is implemented with function $F(x) = x^2$ to try to factor an integer with a prime factor r. Let $\mathrm{ord}_r(x_0) = 2^s t$ where t is odd.

    Find the first values of k and l for which $x_k \equiv x_l \pmod{r}$ in terms of s and the binary expansion of $1/t$. (This will generally be much closer to r than $\sqrt{r}$ in magnitude, which shows that $F(x) = x^2$ is a bad function to use in the Pollard rho algorithm).

28. In the continued fraction expansion of $\sqrt{7}$ as calculated on the previous problem set, let n be such that $a_{n+1} = 2a_0$. Compute the convergent p_n/q_n and show that $x = p_n$, $y = q_n$ gives a solution to Pell's equation $x^2 - 7y^2 = 1$.

29. Evaluate the Legendre symbol $\left(\frac{1801}{8191}\right)$.

30. Let $n > 1$ be an integer. We define a primitive root modulo n to be an integer a such that $\mathrm{ord}_n(a) = \phi(n)$.

    (a) Find a composite integer n which has a primitive root.

    (b) Find a composite integer n for which there are no primitive roots.

31. Let a be an integer not divisible by a prime number p. Suppose that $a^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all primes q which divide $p-1$. Prove that a is a primitive root modulo p.

32. Prove that 3 is a primitive root modulo 65537. (This is exercise 32 of Chapter 3 of Traappe-Washington which contains more hints if you're stuck).

33. Recall the discrete fourier transform: Given a function $F : \mathbb{Z}/N \to \mathbb{C}$, its Fourier transform is a new function $\hat{F} : \mathbb{Z}/N \to \mathbb{C}$ defined by

    $$\hat{F}(\xi) = \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}/N} e^{\frac{2\pi i \xi x}{N}} F(x).$$

    Prove the Fourier inversion formula: $\hat{\hat{F}}(x) = F(-x)$

34. Let p be an odd prime and let g be a primitive root modulo p.

    (a) Let a be an integer not divisible by p. Prove that there exists an integer d such that $g^d \equiv a \pmod{p}$

    (b) Prove that a is a quadratic residue modulo p if and only if the integer d found above is even

    (c) Use this observation to give a proof that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

35. Consider the binary code with four codewords $\{(0,0,1),(1,1,1),(1,0,0),(0,1,0)\}$. Show that this code is not linear and compute its minimum distance.

36. Suppose $k < n + 1 - \log_2(\sum_{i=0}^{d-1} \binom{n}{i})$. Prove that there exists a linear $[n,k,d]$ code.

37. Let k be an integer. There are $2^k - 1$ prisoners. A black or white hat is to be placed on the head of each prisoner. Each prisoner will be able to see the colour of the hats worn by every other prisoner, but not the colour of his or her own hat. From this point in time, no communication between the prisoners is possible. Each prisoner is then simultaneously asked: "What colour is your hat?" There are three allowed responses, white, black and no response. If at least one person guesses their hat colour correctly and noone guesses the wrong colour, the prisoners are set free. Otherwise they are all executed.

    The prisoners may meet beforehand to decide on their strategy. What is their best course of action? Assume that their common goal is to be freed.

38. [10 points] Two possible definitions of ISBN numbers are

    (a) Strings $a_1a_2\cdots a_{10}$ such that $a_1 + 2a_2 + \cdots + 9a_9 + 10a_{10} \equiv 0 \pmod{11}$,

    (b) Strings $a_1a_2\cdots a_{10}$ such that $10a_1 + 9a_2 + \cdots + 2a_9 + a_{10} \equiv 0 \pmod{11}$.

    Prove that these two definitions are equivalent. (ie, a string is an ISBN number under the first definition if and only if it is an ISBN number under the second defition).

39. [10 points] Find an integer solution (x,y) to the equation $-21x + 13y = 1$.

40. [5 points each] For each of the following equations (or system of equations), give the number of solutions. (Your answer should be of the form: There are d solutions modulo N for some d and N.)

    (a) $x^{70} \equiv 1 \pmod{71}$

    (b) $25x + 31 \equiv 121 \pmod{746}$

    (c) $x \equiv 34 \pmod{58}$ and $x \equiv 2 \pmod{100}$.

    (d) $x^2 \equiv 4 \pmod{77}$

41. Find all solutions to the congruence

$$x^2 \equiv 1 \pmod{707}$$

42. Give the continued fraction expansion of $\frac{85}{512}$, and compute all of the partial convergents.

43. Let C be a binary code of length n and minimum distance d. Define a new code C' of length $n+1$ by

$$C' = \{x_1 x_2 \dots x_{n+1} | x_1 x_2 \dots x_n \in C,\ x_1 + \cdots + x_{n+1} \equiv 0 \pmod 2\}$$

Suppose that d is odd. Prove that the minimum distance of C' is $d+1$.

44. Let C be the binary linear code with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

(a) Give a complete list of all the codewords of C.

(b) What is the minimum distance of C? How many errors can it correct?

(c) Decode the words 1100111, 0010110.

45. (a) Jamie and Cercei want to agree on a secret key using a Diffie-Hellman key exchange. They agree to work module the prime 13, with the primitive root 2 being used as the base of the exponent.

If Jamie chooses 3 as his secret exponent and Cercei chooses 10, then what is their resulting shared secret? Give your answer in the form of an integer between 0 and 13.

(b) Prove that in any Diffie-Hellman key exchange (working modulo a prime) an eavesdropper will always be able to determine whether or not the shared secret is a quadratic residue.

46. Let a be an integer.

(a) Prove that

$$\gcd(a-1, a^2+a+1) = \begin{cases} 3 & \text{if } a \equiv 1 \pmod 3 \\ 1 & \text{otherwise} \end{cases}$$

(b) Let $p \neq 3$ be a prime number dividing a^2+a+1. By showing $\mathrm{ord}_p(a) = 3$ or otherwise, prove that $p \equiv 1 \pmod 3$.

47. Consider the following algorithm which takes as input three positive integers a, d, n. Set $y = 1$. While $d \neq 0$:

- if d is even: $a = a^2 \pmod n$, $d = \frac{d}{2}$
- if d is odd: $y = ay \pmod n$, $a = a^2 \pmod n$, $d = \frac{d-1}{2}$

Return y.

(a) Prove that this algorithm computes the value of $a^d \pmod n$.

(b) For this part, assume that $a < n$. What is the runtime of this algorithm? You may express your answer using big O notation.