CS215: Discrete Math (H)
2023 Fall Semester Written Assignment # 3
Due: Nov. 13th, 2023, please submit at the beginning of class

Q.1 What are the prime factorizations of

(a) 12!

(b) 6560

Q.2

(a) Give the prime factorization of 312.

(b) Use Euclidean algorithm to find $\gcd(312, 97)$.

(c) Find integers s and t such that $\gcd(312, 97) = 312s + 97t$.

(d) Solve the modular equation

$$312x \equiv 3 \pmod{97}.$$

Q.3 Prove the following statement: Suppose that $\gcd(b, a) = 1$. Prove that $\gcd(b + a, b - a) \leq 2$.

Q.4 Prove that there exist two powers of 2 that differ by a multiple of 222. That is, prove that there exist two positive integers x and y, such that 222 divides $2^y - 2^x$.

Q.5 Given an integer a, we say that a number n passes the "Fermat primality test (for base a)" if $a^{n-1} \equiv 1 \pmod{n}$.

(a) For $a = 2$, does $n = 561$ pass the test?

(b) Did the test give the correct answer in this case?

Q.6 Let a and b be positive integers. Show that $\gcd(a, b) + \mathrm{lcm}(a, b) = a + b$ if and only if a divides b, or b divides a.

Q.7

(1) Show that there is no integer solution x to the equation

$$x^2 \equiv 31 \pmod{36}.$$

(2) Find the integer solutions x to the system of equations

$$\begin{cases} x^2 \equiv 10 \pmod{31}, \\ x^2 \equiv 30 \pmod{37}. \end{cases}$$

Q.8 Prove that if a and m are positive integers such that $\gcd(a, m) \neq 1$ then a does *not* have an inverse modulo m.

Q.9 Convert the decimal expansion of each of these integers to a binary expansion.

(a) 321 (b) 1023 (c) 100632

Q.10 Suppose that p, q and r are distinct primes. Show that there exist integers a, b and c, such that

$$a(pq) + b(qr) + c(rp) = 1.$$

Q.11 From Google's Corporate Information Page:
"1997 – Larry (Page) and Sergey (Brin) decide that the BackRub search engine needs a new name. After some brainstorming, they go with Google – a play on the word ' googol', a mathematical term for the number represented by the numeral 1 followed by 100 zeros. The use of the term reflects their mission to organize a seemingly infinite amount of information on the web."

The name ' googol' for 10^{100} was coined (around 1920) by a nine-year old child. He also called 10^{googol} a ' googolplex'. Accordingly, Googleplex is the name of Google's headquarters complex in California.

What is the remainder of a googol to a googol modulo 13, i.e., $(10^{100})^{(10^{100})} \bmod 13$?

Q.12 Let the coefficients of the polynomial $f(n) = a_0 + a_1 n + a_2 n^2 + \cdots + a_{t-1} n^{t-1} + n^t$ be integers. We now show that ***no*** non-constant polynomial can generate only prime numbers for integers n. In particular, let $c = f(0) = a_0$ be the constant term of f.

(1) Show that $f(cm)$ is a multiple of c for all $m \in \mathbb{Z}$.

(2) Show that if f is non-constant and $c > 1$, then as n ranges over the nonnegative integers $\mathbb{N}$, there are infinitely many $f(n) \in \mathbb{Z}$ that are not primes. [Hint: You may assume the fact that the magnitude of any non-constant polynomial $f(n)$ grows unboundedly as n grows.]

(3) Conclude that for every non-constant polynomial f there must be an $n \in \mathbb{N}$ such that $f(n)$ is not prime. [Hint: Only one case remains.]

Q.13 Show that $\log_2 3$ is an irrational number. Recall that an irrational number is a real number x cannot be written as the ratio of two integers.

Q.14 Show that if a and m are relatively prime positive integers, then the inverse of a modulo m is unique modulo m.

Q.15 Prove that there are infinitely many primes of the form $4k + 3$, where k is a nonnegative integer. [Hint: Suppose that there are only finitely many such primes $q_1, q_2, \ldots, q_n$, and consider the number $4q_1q_2 \cdots q_n - 1$.]

Q.16

(a) Use Fermat's little theorem to compute $5^{2003} \bmod 7$, $5^{2003} \bmod 11$, and $5^{2003} \bmod 13$.

(b) Use your results from part (a) and the Chinese remainder theorem to find $5^{2003} \bmod 1001$. (Note that $1001 = 7 \cdot 11 \cdot 13$.)

Q.17 Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime integers greater than or equal to 2. Show that if $a \equiv b \pmod{m_i}$ for $i = 1, 2, \ldots, n$, then $a \equiv b \pmod{m}$, where $m = m_1m_2 \cdots m_n$.

Q.18 Show that the simultaneous solution of a system of linear congruences modulo pairwise relatively prime moduli is *unique* modulo the product of these moduli.

Q.19 Find all solutions, if any, to the system of congruences $x \equiv 5 \pmod{6}$, $x \equiv 3 \pmod{10}$, and $x \equiv 8 \pmod{15}$.

Q.20 Recall how the *linear congruential method* works in generating pseudorandom numbers: Initially, four parameters are chosen, i.e., the modulus m, the multiplier a, the increment c, and the seed x_0. Then a sequence of numbers $x_1, x_2, \ldots, x_n, \ldots$ are generated by the following congruence

$$x_{n+1} = (ax_n + c) \pmod{m}.$$

Suppose that we know the generated numbers are in the range $0, 1, \ldots, 10$, which means the modulus $m = 11$. By observing three consecutive numbers $7, 4, 6$, can you predict the next number? Explain your answer.

Q.21 Recall that Euler's totient function $\phi(n)$ counts the number of positive integers up to a given integer n that are coprime to n. Let $m, n \geq 2$ be positive integers such that $m|n$. Prove that $\phi(m)|\phi(n)$ and that $\phi(mn) = m\phi(n)$.

Q.22 Show that we can easily factor n when we know that n is the product of two primes, p and q, and we know the value of $(p-1)(q-1)$.

Q.23 Consider the RSA encryption method. Let our public key be $(n, e) = (65, 7)$, and our private key be d.

(a) What is the encryption $\hat{M}$ of a message $M = 8$?

(b) To decrypt, what value d do we need to use?

(c) Using d, run the RSA decryption method on $\hat{M}$.

Q. 24 Consider the RSA system. Let (e, d) be a key pair for the RSA. Define

$$\lambda(n) = \text{lcm}(p-1, q-1)$$

and compute $d' = e^{-1} \bmod \lambda(n)$. Will decryption using d' instead of d still work? (prove $C^{d'} \bmod n = M$)