Practice Problems

I will try to update this file from time to time throughout the semester to add new problems and some solutions (if I have enough time for that). There might be too many typos and mistakes in the solutions, or even in the problems. Please let me know if you spot a very big mistake.

This is the last update August 9, 2022

1. For which integers n, the expression $\frac{5n^2+6n+4}{3n+2}$ is an integer?

2. Prove that if the integers a, b, c satisfy $9 \mid a^3 + b^3 + c^3$, then they also satisfy $3 \mid abc$.

3. Let $g > 0$ and s be given integers. Prove that there exist integers x and y satisfying $\gcd(x, y) = g$ and $xy = s$ if and only if $g^2 \mid s$.

4. Using Euclid's algorithm, find $\gcd(1378, 1259)$ and integers x, y satisfying $1378x + 1259y = \gcd(1378, 1259)$.

5. Find all the possible values of $\gcd(2n - 1, 9n + 4)$ for integer n.

6. Find $\gcd(2^{19} + 1, 2^{96} + 1)$.

7. Show that $n! + 1$ and $(n + 1)! + 1$ are coprime for integers $n \geq 1$.

8. Find all integer solutions to the linear diophantine equation $1990x + 173y = 11$.

9. Find all integer solutions to the linear diophantine equation $6x + 10y - 15z = 1$.

10. Let a and b be coprime positive integers. Prove that the linear diophantine equation $ax + by = c$ has a solution in non-negative integers for every integer $c \geq (a - 1)(b - 1)$.

11. For which integer(s) n both of the numbers n and $n^2 + 2$ are primes?

12. Find the smallest positive integers a and b satisfying $2a^2 = 3b^3$.

13. Find the integer values of n for which $n(n + 17)$ is the square of an integer.

14. Prove that there are infinitely many primes of the form $3k + 2$.

15. A positive integer n is called *powerful* if for every prime p dividing n, p^2 also divides n. Prove that a positive integer n is powerful if and only if it can be expressed as $n = a^2b^3$ for some positive integers a and b.

16. Prove for the positive integers a, b, c that

$$\gcd(a, b, c) \cdot \operatorname{lcm}[ab, bc, ca] = abc.$$

17. Let n be a positive integer. Prove that there are infinitely many primes p with the sum of its digits larger than n.

18. The last k digits of 2^n are equal. Prove that $k \leq 3$.

19. Let $n \geq 0$ be an integer, then prove that $2^{n+2} \| 5^{2^n} - 1$.

20. Let $p(x)$ be a polynomial with integer coefficients.

(a) Prove for distinct integers a and b that $a - b \mid p(a) - p(b)$.

(b) Suppose three distinct integers a, b, c satisfy $p(a) = p(b) = p(c) = 1$. Prove for every integer n that $p(n) \neq 0$.

21. For a real number x, let $\lfloor x \rfloor$ denote the largest integer less than or equal to x. Let n be a positive integer and p be a prime such that $p^e \| n!$, then prove that

$$e = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots .$$

22. Find all prime numbers p such that $|p^4 - 86|$ is also a prime.

23. Prove that the equation $a_1^4 + a_2^4 + \cdots + a_{14}^4 = 160015$ has no integer solutions $(a_1, a_2, \cdots, a_{14})$.

24. Find all integer solutions to $x^2 + y^2 = 3z^2$ (Hint: Start with cancelling out $\gcd(x, y, z)$ if it is not equal to 1 already).

25. Prove that $a \equiv b \mod n \Longrightarrow \gcd(a, n) = \gcd(b, n)$.

26. Let a, b, n, and k be positive integers such that $\gcd(a, n) = 1$. Prove that

$$a^k \equiv b^k \pmod{n} \text{ and } a^{k+1} \equiv b^{k+1} \pmod{n} \Longrightarrow a \equiv b \pmod{n}.$$

Would it be still true without $\gcd(a, n) = 1$?

27. Prove for every integer n that $30 \mid n^5 - n$.

28. Find an integer n such that all of the last three digits of n^2 are equal to 4. Is there an integer n such that all of the last four digits of n^2 are equal to 4?

29. Find the three smallest positive integer values of x satisfying all of the congruences

$$\begin{aligned} n &\equiv 2 \pmod{3} \\ n &\equiv 4 \pmod{5} \\ n &\equiv 6 \pmod{7} \\ n &\equiv 10 \pmod{11}. \end{aligned}$$

30. How many solutions does the congruence $x^3 \equiv 1 \pmod{273}$ has in $\mathbb{Z}_{273}$?

31. Some integers $a_1, a_2, \cdots, a_{1013}$ are given. Prove that we can always find some $i \neq j$ such that $a_i \equiv a_j \pmod{2022}$ or $a_i = -a_j \pmod{2022}$.

32. Let m be a positive integer. A set of m integers, containing one representative from each of the m congruence classes in $\mathbb{Z}_m$ is called a *complete set of residues modulo m*. Suppose $\{r_0, r_1, \cdots, r_{m-1}\}$ is a complete residue system modulo m. Prove that

$$r_0 + r_1 + \cdots + r_{m-1} \equiv \begin{cases} 0 \pmod{m} & \text{if m is odd} \\ \frac{m}{2} \pmod{m} & \text{if m is even.} \end{cases}$$

33. Let c be a positive integer and $\{r_0, r_1, \cdots, r_{m-1}\}$ be a complete residue system modulo m. Prove that $\{cr_0, cr_1, \cdots, cr_{m-1}\}$ is also a complete residue system modulo m if and only $\gcd(c, m) = 1$.

34. Recall that (a, n) depends only on the congrunce class of a in $\mathbb{Z}_n$ (for example, see Question 25).

(a) For a prime p and a positive integer k, prove that $\gcd(a, p^k) = 1$ for exactly $p^{k-1} \cdot (p-1)$ values of a in $\mathbb{Z}_{p^k}$.

(b) Let $n \geq 2$ be a positive integer with the prime factorisation $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Using the previous part and the Chinese Remainder Theorem, deduce that the number of the integers $1 \leq a \leq n$ satisfying $\gcd(a, n) = 1$ is

$$\phi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1} \cdot (p_i - 1).$$

35. Let p be a prime and n is an arbitrary positive integer. Prove that $n^p + n \cdot (p-1)!$ is divisible by p.

36. Find $0 \leq a \leq 6$ such that

$$10^{10^0} + 10^{10^1} + 10^{10^2} + \cdots + 10^{10^{10}} \equiv a \pmod 7.$$

37. Prove that if 7 divides the 2022-digit integer $\overline{a_1 a_2 \cdots a_{2022}}$, then it also divides $\overline{a_{2022} a_1 a_2 \cdots a_{2021}}$.

38. Find all positive integers n such that $n^5 + 5^n \equiv 0 \pmod{11}$.

39. Let p be a prime. Prove that $(p-2)! \equiv 1 \pmod p$ and $(p-3)! \equiv \frac{p-1}{2} \pmod p$.

40. Suppose q is a prime such that $7 \cdot 23 \cdot q$ is a Carmichael number. Find q.

41. Prove that 25 passes base 7-test, i.e. $7^{25} \equiv 7 \pmod{25}$.

42. Suppose an integer n passes the base a-test and the base b-test, prove that it also passes the base ab-test.

43. Suppose an integer n passes the base a-test while failing the base b-test, prove that it also fails the base ab-test if $\gcd(a, n) = 1$. Give a counter-example for the case $\gcd(a, n) \neq 1$.

44. Solve the congruence

$$x^3 + 3x^2 + x + 3 \equiv 0 \pmod{25}$$

in $\mathbb{Z}_{25}$.

45. Let $n \geq 2$. Prove that the number of the units of $\mathbb{Z}_n$ is even unless $n = 2$.

46. Find all positive integers n satisfying $\phi(n) = 20$.

47. Prove that there is no n satisfying $\phi(n) = 14$.

48. Prove for any odd integer n that $n^{33} \equiv n \pmod{4080}$.

49. Prove that every positive integer n with $\gcd(n, 10) = 1$ divides infinitely many terms of the sequence

$$1, 11, 111, 1111, 11111, \ldots.$$

50. Find all primitive roots of $\mathbb{Z}_{17}$.

51. Let p be an odd prime and g be primitive root modulo p. Show that $-g$ is a primitive root modulo p if and only if $p \equiv 1 \pmod 4$.

52. Let n be a positive integer. Prove that $n \mid \phi(2^n - 1)$

53. Let p be a prime. If $\mathrm{ord}_p(u) = 3$, then show that $u^2 + u + 1 \equiv 0 \pmod p$ and that $\mathrm{ord}_p(1 + u) = 6$.

54. Let p be prime and g be a primitive root modulo p^2. Show that g is also a primitive root modulo p.

55. Let n be a positive integer such that $\mathbb{Z}_n$ has a primitive root and let a be a unit modulo n. Show that the congruence

$$x^k \equiv a \pmod n$$

has a solution if and only if

$$a^{\frac{\phi(n)}{\gcd(k,\phi(n))}} \equiv 1 \pmod n.$$

56. Find the number of the solutions to the congruence $x^4 \equiv 61 \pmod{117}$ in $\mathbb{Z}_{117}$.

57. (a) Which primes p satisfy $\left(\frac{-2}{p}\right) = 1$?

(b) Which primes satisfy $\left(\frac{7}{p}\right) = 1$?

58. Compute the Legendre symbol $\left(\frac{814}{2003}\right)$.

59. (a) Prove for prime $p > 3$ that the sum of all quadratic residues of $\mathbb{Z}_p$ is equivalent to $0 \pmod p$.

(b) Prove for prime $p \neq 2$ that the product of all quadratic residues of $\mathbb{Z}_p$ is equivalent to $(-1)^{\frac{p+1}{2}} \pmod p$.

60. Let $p \equiv 3 \pmod 4$ and n is a positive integer. Show that $\frac{p+1}{4} + n(n+1)$ is either divisible by p or it is a quadratic residue modulo p.

61. Let p be a prime. Prove that if the congruence

$$x^2 - x + 3 \equiv 0 \pmod p$$

has a solution, then so is the congruence

$$y^2 - y + 25 \equiv 0 \pmod p.$$

62. (a) Show that a prime divisor p of $4n^2 + 3$ is either $p = 3$ or $p \equiv 1 \pmod 3$.

(b) Prove that there are infinitely many primes of the form $3k + 1$.

63. Is 43 quadratic residue modulo 923? If yes, then find the number of solutions to the congruence $x^2 \equiv 43 \pmod{923}$ in $\mathbb{Z}_{923}$.

64. (This is hard) Let $p \neq 2$ be a prime. Prove that there exists an integer a such that $1 \leq a \leq 1 + \sqrt{p}$ and $\left(\frac{a}{p}\right) = -1$, in other words the smallest quadratic non-residue modulo p cannot be larger than $1 + \sqrt{p}$.