Modular Arithmetic and Residue Classes

6 June 2020

Problem 1. Prove that there are infinitely many primes of the form $4k - 1$; that is, congruent to 3 modulo 4.

Problem 2. [Baltic 2001] Let a be an odd integer. Prove that $a^{2^n} + 2^{2^n}$ and $a^{2^m} + 2^{2^m}$ are relatively prime for all positive integers n and m with $n \neq m$.

Problem 3. Let m be an even positive integer. Assume that

$$\{a_1, a_2, \ldots, a_m\} \quad \text{and} \quad \{b_1, b_2, \ldots, b_m\}$$

are two complete sets of residue classes modulo m. Prove that

$$\{a_1 + b_1, a_2 + b_2, \ldots, a_m + b_m\}$$

is not a complete set of residue classes.

Problem 4. Let a be a positive integer. Determine all the positive integers m such that

$$\{a \cdot 1, a \cdot 2, a \cdot 3, \ldots, a \cdot m\}$$

is a set of complete residue classes modulo m.

Problem 5. Let m be a positive integer. Let a be an integer relatively prime to m, and let b be an integer. Assume that S is a complete set of residue classes modulo m. The set

$$T = aS + b = \{as + b \mid s \in S\}$$

is also a complete set of residue classes modulo n.

Problem 6. Let m be a positive integer. Let a be an integer relatively prime to m, and let b be an integer. There exist integers x such that $ax \equiv b \pmod{m}$, and all these integers form exactly one residue class modulo m.

Problem 7. Let m be a positive integer, and let a and b be integers relatively prime to m. If x and y are integers such that

$$a^x \equiv b^x \pmod{m} \quad \text{and} \quad a^y \equiv b^y \pmod{m},$$

then

$$a^{\gcd(x,y)} \equiv b^{\gcd(x,y)} \pmod{m}.$$

Problem 8. [Wilson's Theorem] For any prime p, $(p-1)! \equiv -1 \pmod{p}$.

Problem 9. [Bézout] For positive integers m and n, there exist integers x and y such that $mx + ny = \gcd(m, n)$.

Problem 10. Let m be a positive integer, and let a and b be integers relatively prime to m. If x and y are integers such that

$$a^x \equiv b^x \pmod{m} \quad \text{and} \quad a^y \equiv b^y \pmod{m},$$

then

$$a^{\gcd(x,y)} \equiv b^{\gcd(x,y)} \pmod{m}.$$

Fermat's Little Theorem and Euler's Theorem

7 June 2020

11. Fermat's little theorem. Let p be a prime number.

(a) Show that if k is an integer with $0 < k < p$, then $\binom{p}{k}$ is divisible by p.

(b) Show that if $a \in \mathbb{Z}$, then $(a+1)^p \equiv a^p + 1 \pmod{p}$.

(c) Show that if $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$.

(d) Show that if a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

12. Another look at Fermat's little theorem. Let p be a prime number, and a an integer not divisible by p.

(a) Show that $\{a, 2a, 3a, \ldots, (p-1)a\} \equiv \{1, 2, 3, \ldots, p-1\} \pmod{p}$.

(b) Show that $a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod{p}$.

(c) Conclude that $a^{p-1} \equiv 1 \pmod{p}$.

13. Euler's totient function. We use $\phi(n)$ to denote the number of elements in $\{1, 2, \ldots, n\}$ that are relatively prime to n. That is, $\phi(n) = |\mathbb{Z}_n^*|$.

(a) Compute $\phi(7)$ and $\phi(24)$.

(b) Compute $\phi(p^n)$, where p is a prime and n is a positive integer.

(c) Show that if m and n are relatively prime integers, then $\phi(mn) = \phi(m)\phi(n)$.

(d) Find a formula for computing $\phi(n)$ in terms of the prime factorization of n.

Euler's Theorem and Problems on Divisibility

8 June 2020

Some review problems from last homework:

14. (a) Let p be a prime number. Determine the greatest power of p that divides $n!$, where n is a positive integer.

(b) Let m and n be positive integers. Show that $\dfrac{(m+n)!}{m!n!}$ is an integer (without referring to binomial coefficients).

15. (USAMO 1972) Show that

$$\frac{\gcd(a,b,c)^2}{\gcd(a,b)\gcd(b,c)\gcd(c,a)} = \frac{\operatorname{lcm}(a,b,c)^2}{\operatorname{lcm}(a,b)\operatorname{lcm}(b,c)\operatorname{lcm}(c,a)}.$$

16. (a) Show that if a and b are relatively prime integers, then $\gcd(a+b, a^2-ab+b^2) = 1$ or 3.

(b) Show that if a and b are relatively prime integers, and p is an odd prime, then

$$\gcd\left(a+b, \frac{a^p+b^p}{a+b}\right) = 1 \text{ or } p.$$

17. Let n be a positive integer.

(a) Find n consecutive composite numbers.

(b) Find n consecutive positive integers, none of which is a power of a prime.

Class Problems:

18. Euler's Theorem Let a and m be relatively prime integers.

(a) Let $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ be the set of positive integers less than m and relatively prime to m. Show that

$$\{r_1, r_2, \ldots, r_{\phi(n)}\} \equiv \{ar_1, ar_2, \ldots, ar_{\phi(n)}\} \pmod{m}.$$

(b) Show that $a^{\phi(m)} \equiv 1 \pmod{m}$.

Problem 19. [IMO 2005] Consider the sequence $a_1, a_2, \ldots$ defined by

$$a_n = 2^n + 3^n + 6^n - 1$$

Problem 20. Find an infinite nonconstant arithmetic progression of positive integers such that each term is not a sum of two perfect cubes.

Order of an Element and Problems on Residue Classes and Euler's Theorem

9 June 2020

Problem 21. [IMO 2003 shortlist] Determine the smallest positive integer k such that there exist integers $x_1, x_2, \ldots, x_k$ with

$$x_1^3 + x_2^3 + \cdots + x_k^3 = 2002^{2002}.$$

Problem 22. [Gauss] For any positive integer n,

$$\sum_{d|n} \varphi(d) = n.$$

Some review problems from last homework:

23. RSA public-key cryptography. Alice and Bob are sending cryptic messages to each other. Let p and q be distinct primes and $n = pq$ and $t = (p-1)(q-1)$. Let e, d be positive integers such that $ed \equiv 1 \pmod t$. Alice takes a message, M (an integer relatively prime to n, and sends $C = M^e$ to Bob. Bob receives C and computes $M' = C^d \pmod n$. Prove that $M \equiv M' \pmod n$.

24. Let m be an even positive integer. Assume that

$$\{a_1, a_2, \ldots, a_m\} \quad \text{and} \quad \{b_1, b_2, \ldots, b_m\}$$

are two complete sets of residue classes modulo m. Prove that

$$\{a_1 + b_1, a_2 + b_2, \ldots, a_m + b_m\}$$

is not a set of complete residue classes.

25. Let $p \geq 3$ be a prime, and let

$$\{a_1, a_2, \ldots, a_p\} \quad \text{and} \quad \{b_1, b_2, \ldots, b_p\}$$

be two sets of complete residue classes modulo p. Prove that

$$\{a_1 b_1, a_2 b_2, \ldots, a_p b_p\}$$

is not a complete set of residue classes modulo p.

26. Find all non-negative integer solutions to $4ab - a - b = c^2$.

27. For an odd positive integer $n > 1$, let S be the set of integers x, $1 \leq x \leq n$, such that both x and $x + 1$ are relatively prime to n. Show that $\prod_{x \in S} x \equiv 1 \pmod n$.

Problems on Order of an Element:

28. Let $m > 1$ be a positive integer, and let a be an integer relatively prime to m. Show that there is a least positive integer d for which $a^d \equiv 1 \pmod{m}$.

We say that d is the *order* of a modulo m, denoted by $\mathrm{ord}_m(a)$ or simply $\mathrm{ord}(a)$ is the modulus m is understood.

29. Let m be a positive integer, and a an integer relatively prime to m.

(a) Show that $a^n \equiv 1 \pmod{m}$ if and only if $\mathrm{ord}_m(a) \mid n$.

(b) Furthermore, show that $a^{n_0} \equiv a^{n_1} \pmod{m}$ if and only if $\mathrm{ord}_m(a) \mid n_0 - n_1$.

(c) Show that $\mathrm{ord}_m(a) \mid \phi(m)$.

Problems on Order of an Element

10 June 2020

Homework Problems (Order of an Element):

30. Show that the order of 2 modulo 101 is 100.

31. Prove that for all positive integers $a > 1$ and n, we have $n \mid \phi(a^n - 1)$.

32. Prove that if p is a prime, then every prime divisor of $2^p - 1$ is greater than p.

33. Prove that if p is a prime, then $p^p - 1$ has a prime factor of the form $kp + 1$.

34. Let a and $b > 2$ be positive integers. Show that $2^a + 1$ is not divisible by $2^b - 1$.

More Problems on Order of an Element:

Problem 35. (AIME 2001). *How many positive integer multiples of 1001 can be expressed in the form $10^j - 10^i$, where i and j are integers and $0 \leq i < j \leq 99$?*

Problem 36. . *Let p be an odd prime, and let q and r be primes such that p divides $q^r + 1$. Prove that either $2r \mid p - 1$ or $p \mid q^2 - 1$.*

Problems on Order of an Element 2

11 June 2020

More Problems on Order of an Element:

Problem 37. *Let* $a > 1$ *and* n *be given positive integers. If* p *is an odd prime divisor of* $a^{2^n} + 1$*, prove that* $p - 1$ *is divisible by* 2^{n+1}.

Problem 38. (Classical). *Let* n *be an integer with* $n \geq 2$. *Prove that* n *doesn't divide* $2^n - 1$.

Problem 39. *Let* a *and* b *be relatively prime integers. Prove that any odd divisor of* $a^{2^n} + b^{2^n}$ *is of the form* $2^{n+1}m + 1$.

Problem 40. (Bulgaria 1996). *Find all pairs of prime* p, q *such that* $pq \mid (5^p - 2^p)(5^q - 2^q)$.

Problem 41. (USA TST 2003). *Find all ordered prime triples* (p, q, r) *such that* $p \mid q^r + 1$, $q \mid r^p + 1$, *and* $r \mid p^q + 1$.

Problem 42. *Prove that for* $n > 1$ *we have* $n \nmid 2^{n-1} + 1$.

Problem 43. *(China 2009) Find all pairs of primes* p, q *such that*

$$pq \mid 5^p + 5^q$$

Problems on Order of an Element 3

13 June 2020

More Problems on Order of an Element:

Problem 44. *Let q be fixed prime number. Show that there exists infinitely many primes of the form $qm+1$*

Problem 45. *Calculate $ord_{3^n}(2)$ for any $n \in \mathbb{N}$.*

Problem 46. *Find all pairs of prime numbers (p,q) such that $\frac{(2p^2-1)^q+1}{p+q}$ and $\frac{(2q^2-1)^p+1}{p+q}$ are integers*

Problem 47. *Let k, n be positive integers greater than 1. Prove that if there exists natural number a such that $k|2^a+1$, $n|2^a-1$ then there is no natural number b satisfying $k|2^b+1$, $n|2^b-1$.*

Problem 48. *When $3|p-2$ show that $a^3 \equiv b^3 (mod\ n)$ if and only if $a \equiv b\ (mod\ n)$.*

Problem 49. *When $\gcd(p-1,k)=1$ show that $a^k \equiv b^k (mod\ n)$ if and only if $a \equiv b\ (mod\ n)$.*

Problem 50. (Balkan MO 1999). *Let $p>2$ be a prime number such that $3|(p-2)$. Let*

$$S=\{y^2-x^3-1 | 0 \leq x,y \leq p-1 \cap x,y \in \mathbb{Z}\}$$

Prove that there are at most p elements of S divisible by p.

Problems on Chinese Remainder Theorem

13 June 2020

Problem 51 (Chinese Remainder Theorem). *The system of linear congruences*

$$\begin{cases} x \equiv a_1 \pmod{b_1}, \\ x \equiv a_2 \pmod{b_2}, \\ \cdots \\ x \equiv a_n \pmod{b_n}, \end{cases}$$

where $b_1, b_2, \cdots, b_n$ are pairwise relatively prime (aka $\gcd(b_i, b_j) = 1$ iff $i \neq j$) has one distinct solution for x modulo $b_1 b_2 \cdots b_n$.

Problem 52 (AIME II 2012). *For a positive integer p, define the positive integer n to be p-safe if n differs in absolute value by more than 2 from all multiples of p. For example, the set of 10-safe numbers is $3, 4, 5, 6, 7, 13, 14, 15, 16, 17, 23, \ldots$. Find the number of positive integers less than or equal to $10,000$ which are simultaneously 7-safe, 11-safe, and 13-safe.*

Problem 53 (AOPS). *Show that for $c \in \mathbb{Z}$ and a prime p, the congruence $x^x \equiv c \pmod{p}$ has a solution.*

Problem 54 (ISL 2005 N6). *Let a, b be positive integers such that $b^n + n$ is a multiple of $a^n + n$ for all positive integers n. Prove that $a = b$.*

Homework Problems:

Problem 55. (USAMO 1991). *Show that, for any fixed integer $n \geq 1$, the sequence*

$$2,\ 2^2,\ 2^{2^2},\ 2^{2^{2^2}}, \ldots \pmod{n}$$

is eventually constant.

[The tower of exponents is defined by $a_1 = 2$, $a_{i+1} = 2^{a_i}$. Also $a_i \pmod{n}$ means the remainder which results from dividing a_i by n.]

Problem 56. (Korea 1999). *Find all positive integers n such that $2^n - 1$ is a multiple of 3 and $(2^n - 1)/3$ is a divisor of $4m^2 + 1$ for some integer m.*