INDIAN STATISTICAL INSTITUTE
Bangalore Centre

Problem Set

BMath: Autumn Semester, 2024.
Course: *Elementary Number Theory* (B4).
Instructor: Ramdin Mawia.
Last updated: 2024/10/19 at 12:07.
Due date: ∞

Elementary Number Theory

Induction

1. Use induction to prove the *Binomial Theorem*:

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^j y^{n-j}$$

for all positive integers $n \geqslant 1$ and all commuting variables x and y.

2. Use induction to prove the identity $\sum_{k=1}^{n} k!k = (n+1)! - 1$ for all $n \geqslant 1$.

3. Use induction argument to prove that $\sum_{k=1}^{n} 1/k^2 \leqslant 2 - 1/n$ for all $n \geqslant 1$.

4. Let θ be a real number. Write $p_0 = 1, p_1 = \cos\theta$ and define $p_{n+1} = 2p_1p_n - p_{n-1}$ for $n \geqslant 1$. Use induction to prove that $p_n = \cos n\theta$ for $n \geqslant 0$.

5. The *Fibonacci sequence* $\{F_n\}_{n\geqslant 0}$ is defined by $F_0 = 0, F_1 = 1$ and $F_{n+1} = F_{n-1} + F_n$ for $n \geqslant 1$. Use induction to prove that

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

holds for all $n \geqslant 0$.

Divisibility

6. Use induction to show the following:

   (a) $8 | 5^{2n} + 7$ for $n \geqslant 1$.

   (b) $21 | 4^{n+1} + 5^{2n-1}$ for $n \geqslant 1$.

7. For any integer a show that $2|a(a+1), 3|(a-1)a(a+1), 3|a(2a^2+7)$.

8. For an odd integer a, the integer $a^2+(a+2)^2+(a+4)^2+1$ is divisible by 12.

9. The product of any three consecutive integers is divisible by $6 = 3!$, the product of any four consecutive integers is divisible by $24 = 4!$ and the product of any k consecutive integers is divisible by $k!$

GCD

10. If $\gcd(a,b)=1$ and $\gcd(a,c)=1$ then $\gcd(a,bc)=1$.

11. If $\gcd(a,b)=1$ then $\gcd(a^k,b^\ell)=1$ for any $k,\ell \geqslant 0$.

12. If $a|bc$ then $a|\gcd(a,b)\gcd(a,c)$.

Congruences

13. Show that $7|5^{2020}+3\cdot 2^{5048}$.

14. Show that $43|6^{n+2}+7^{2n+1}$ for any integer $n \geqslant 1$.

15. Find the last digit of 3^{2021}.

Chinese Remainder Theorem

16. A basket contains a certain number of eggs. If the eggs are sold in packs of 3, one egg remains; if they are sold in packs of 5, two eggs remain, and if they are sold in packs of 7, three eggs remain. What is the minimum number of eggs in the basket?

17. Solve the following simultaneous congruences:

(a) $$\begin{aligned} x &\equiv 1 \pmod{3},\\ x &\equiv 3 \pmod{5},\\ x &\equiv 5 \pmod{7}.\end{aligned}$$

(b) $$\begin{aligned} x &\equiv 5 \pmod{11},\\ x &\equiv 7 \pmod{13},\\ x &\equiv 11 \pmod{17}.\end{aligned}$$

(c) $$\begin{aligned} 2x &\equiv 1 \pmod{5},\\ 3x &\equiv 7 \pmod{13},\\ 4x &\equiv 11 \pmod{17}.\end{aligned}$$

Very little Group Theory[1]

18. Define a binary operation $*$ on $\mathbb{Q}^{(1)} = \mathbb{Q}\backslash\{1\}$ by $r * s = r + s - rs$. Prove that $\mathbb{Q}^{(1)}$ is a group under $*$. Is it abelian?

[1] If some of the group theory problems are too difficult, don't waste too much time on them! They will not be needed for the course. This section is just for your practice and fun.

19. Is the group $\mathbb{Z}/m\mathbb{Z}$ cyclic? (Here, as usual, the binary operation is *addition* modulo m.)

20. How many subgroups does $(\mathbb{Z}/13\mathbb{Z})^\times$ have? Describe all of them one by one.

21. Is the group $(\mathbb{Z}/15\mathbb{Z})^\times$ cyclic?

22. Are the following groups cyclic? (Some of them were treated in class, but do recall them for yourselves!) Also, do verify that they indeed form groups under the stated binary operations.

    i. $\mathbb{C}$ under addition.

    ii. The set of *positive* rationals $\mathbb{Q}$ under multiplication.

    iii. The set of all rational numbers of the form a/b where $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$ and $b > 0$ is *odd*. The binary operation here is addition. I will denote this group by $\mathbb{Z}_{(2)}$.

    iv. Let p be a prime. Let $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : (a, b) = 1, b > 0 \text{ and } p \nmid b\}$. Is this a group under addition? Is it cyclic?

    v. Let $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. Show that this is a group under the usual multiplication of complex numbers. Show that it is *not* cyclic in at least two different ways! Prove that it has infinitely many finite cyclic subgroups.

23. Let G be a group (not necessarily abelian nor finite). If $x, y \in G$ are of finite order, is it true that xy is of finite order? (*Hint.* Think of 2×2 real/rational matrices).

24. State true or false:

    i. Any group of prime order is cyclic.

    ii. Every cyclic group is abelian.

    iii. Every abelian group is cyclic.

    iv. Every group has a finite subgroup consisting of at least 2 elements.

    v. If G is a group all of whose elements are of finite order, then G is finite.

RSA Cryptography

25. Decrypt the following encrypted texts, the public keys being: $m = 3573103, k = 997$, and the encoding scheme being $A = 11, B = 12, ..., Z = 36$. [You are allowed to use any computer programme and any programming language to accomplish your task. You have to factorise m and find $\bar{k}$.]

i. 879010”2442544 (the symbol ” separates the blocks). It is a 5-letter word (so 10 digits) which I have split into two blocks of 5 digits each.

ii. 93221”1721846 (the symbol ” separates the blocks). It is a 4-letter word (so 8 digits) which I have split into two blocks of 4 digits each.

26. Decrypt the following encrypted texts, the public keys being: $m = 1189852454939$, $k = 17321$, and the encoding scheme being $A = 11, B = 12, ..., Z = 36$ and space=37. [You are allowed to use any computer programme and any programming language to accomplish your task. You have to factorise m and find $\bar{k}$.]

    i. 545155116413 269419630425 940571232929 181471220805 74232461887 97746545655 (space separates the blocks). It is a sentence with 10 letters and 2 spaces (so $12 \times 2 = 24$ digits) which I have split into blocks of 4 digits, starting from the first.

    ii. 129149337319”1041841470234”269419630425 ”122361988668”1179267442284” 1170643014850 (the symbol ” separates the blocks). It is a sentence with 9 letters and 2 spaces (so $11 \times 2 = 22$ digits) which I have split into blocks of 4 digits each starting from the first, so the last block consists of two digits.

Primitive roots and Quadratic residues

27. If p is an odd prime prove that $1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}$.

28. Find all the incongruent primitive roots of the prime $p = 59$.

29. Find all the incongruent primitive roots of $81 = 3^4$.

30. Solve the following quadratic congruences (or prove that they are not solvable):

    (a) $x^2 + 7x + 10 \equiv 0 \pmod{11}$.

    (b) $3x^2 + 4x + 5 \equiv 0 \pmod{13}$.

31. Evaluate the Legendre symbols $(7/23), (11/29), (6/31), (8/53)$ using Gauss’s Lemma.

32. Evaluate the Legendre symbols $(23/29), (29/23), (-5/127), (20/37), (12345/17321)$, and $(1000981/1000999)$ by any method.

33. Describe all primes p for which 13 is a quadratic nonresidue mod p.

34. Prove that there are infinitely many primes of the form $8k + 1$.

Quadratic congruences

35. Does the quadratic congruence $x^2 \equiv 41 \pmod{100}$ have a solution? What about $x^2 \equiv 67 \pmod{100}$?

36. Solve $x^2 + 5x + 6 \equiv 0 \pmod{125}$.

37. For fixed $n > 1$, show that all solvable congruences $x^2 \equiv a \pmod{n}$ with $\gcd(a, n) = 1$ have the same number of solutions.

38. In continuation of the preceding problem, is it true that all solvable congruences $x^k \equiv a \pmod{n}$ with $\gcd(a, n) = 1$ also have the same number of solutions, where $k \geqslant 2$ is any fixed positive integer? [*Hint.* Did your proof of the above result depend on the power 2? Where did you use its 2-**ness**?]

39. Are the following congruences solvable? If yes, solve them.

    (a) $x^2 \equiv 127 \pmod{317}$.

    (b) $3x^2 + 4x + 5 \equiv 0 \pmod{2021}$.

    (c) $x^2 + x + 1 \equiv 0 \pmod{2020}$.

40. Determine whether each of the following is solvable in integers, and solve them when possible.

    (a) $127x^2 + 317^2 y = 13$.

    (b) $3x^2 + 15y = 22$.

    (c) $3x^2 + 4 = 97y$.

    (d) $x^2 + 14 = 5^3 y$.

    (e) $x^2 + 7^3 y = 2$.

    (f) $x^2 + 11^2 23^2 y = 3$.

Combinatorial Number Theory

41. Prove that, for any prime p, there are integers a and b such that p divides $a^2 + b^2 + 1$.

42. Let p be a prime and a, b be integers such that $p \nmid ab$. Prove that the congruence $aX^2 + bY^2 \equiv c \pmod{p}$ is solvable in integers for any $c \in \mathbb{Z}$.

43. Prove that among any ten consecutive positive integers, at least one is relatively prime to the product of the others.

Binary Quadratic Forms

44. Determine whether the following pairs of binary quadratic forms are properly equivalent or not. If they are properly equivalent, give a matrix which takes one to the other:

- $(1,2,3)$ and $(1,0,2)$
- $(1,0,3)$ and $(3,0,1)$.
- $(3,2,1)$ and $(1,2,3)$.
- $(1,1,3)$ and $(1,-1,3)$.
- $(2,3,4)$ and $(2,-3,4)$.
- $(1,3,10)$ and $(2,3,5)$.

45. Prove that $h(D) = 1$ for each of the following discriminants

$$D \in \{-3,-4,-7,-8,-11,-12,-16,-19,-27,-28,-43,-67,-163\}.$$

46. Compute the class number $h(D)$ for each of the following values of D :

(a) -15.

(b) 13.

(c) 21.

(d) -59.

(e) -100

(f) -47.

47. Find the reduced forms of the following binary quadratic forms:

(a) $(2,6,9)$

(b) $(3,-1,3)$

(c) $(5,5,4)$

(d) $(1,3,3)$

(e) $(2,6,7)$

(f) $(1,0,1)$

48. Let p be a prime and $f(X,Y)$ be a primitive binary quadratic form. Prove that p cannot divide all of $f(0,1)$, $f(1,0)$ and $f(1,1)$. Deduce that if S is a finite set of primes, there are coprime integers x and y such that $p \nmid f(x,y)$ for any $p \in S$.

49. Show that X^2+5Y^2 and $2X^2+2XY+3Y^2$ are the only reduced binary quadratic forms of discriminant -20.

i. Prove that the first of these forms does not represent 2, but that the second one does. Deduce that the class number $h(-20) = 2$.

ii. Show that an odd prime p is represented by at least one of these forms if and only if $p = 5$ or $p \equiv 1, 3, 7, \text{ or } 9 \pmod{20}$.

Arithmetic Functions

50. Compute the following Dirichlet convolutions (you need not get another simple arithmetic function, but try to simplify them as much as possible):

(a) $\sigma * \mu$.

(b) $\tau * \mu$.

(c) $\varphi * \mu$.

(d) $\tau * \varphi$.

(e) $u * \sigma_k$.

(f) $\varphi * \mathbb{1}$.

51. Prove the following:

    (a) $\sum_{d|n} \tau(d)\mu(n/d) = 1$ for every positive integer n (i.e., $\tau * \mu = u$).

    (b) $\sum_{d|n} \sigma(d)\mu(n/d) = n$ for every positive integer n (i.e., $\sigma * \mu = \mathbb{1}$).

    (c) $\mu^2(n) = \sum_{d^2|n} \mu(d)$ for every positive integer n.

    (d)[2] $\lim_{x\to\infty} Q(x)/x = 6/\pi^2$ where $Q(x)$ denotes the number of squarefree positive integers $\leqslant x$. [*Hint.* Use 51c above.]

52. Let $\sigma(n)$ denote, as usual, the sum of the positive divisors of $n \in \mathbb{Z}^+$. Prove the following: **10**

    i. σ is multiplicative but not completely multiplicative.

    ii. $\sigma(n) < n(1 + \log n)$ for all $n \geqslant 2$.

    iii. $\sum_{n\leqslant x} \sigma(n) = (\pi^2/12)x^2 + O(x \log x)$.[3]

53. Let f be a multiplicative arithmetic function. Prove that f is completely multiplicative if and only if $f^{-1} = f\mu$.

54. Prove that
$$\frac{n}{\varphi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)}.$$

55. State the Möbius inversion formula. Use it to show that the following two formulas are equivalent:[5] **10**

    - $\tau(mn) = \sum_{d|(m,n)} \mu(d)\tau(m/d)\tau(n/d)$ for all positive integers m and n.
    - $\tau(m)\tau(n) = \sum_{d|(m,n)} \tau(mn/d^2)$ for all positive integers m and n.

    Here, τ is the usual divisor-counting function.

56. Prove the following:

[2] No problem if you can't solve this!

[3] Here you may need to use the well-known sum $\zeta(2) = \sum_{n\geqslant 1} n^{-2} = \pi^2/6$.

[5] You are ***not*** asked to prove that the two formulas are correct (which they are)!

i. $\prod_{d|n} d = n^{\tau(n)/2}$.

ii. $\sum_{d|n} \tau(d)^3 = \left(\sum_{d|n} \tau(d)\right)^2$.

iii. $\sigma = \varphi * \tau$.

iv. $\sigma_\alpha(m)\sigma_\alpha(n) = \sum_{d|(m,n)} d^\alpha \sigma_\alpha(mn/d^2)$.

Recall that, by definition, $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$ for any $\alpha \in \mathbb{C}$ and so $\sigma = \sigma_1, \tau = \sigma_0$.

57. Using Euler-Maclaurin summation formula or otherwise, prove the following:

i. $\log[x]! = x\log x - x + O(\log x)$ for $x \geqslant 2$.

ii. $\sum_{n\leqslant x} 1/n^s = x^{1-s}/(1-s) + \zeta(s) + O(x^{-s})$ for any real $s > 0, s \neq 1$, where $\zeta(s)$ is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \text{if } s > 1,$$

and by

$$\zeta(s) = \lim_{x\to\infty} \left(\sum_{n\leqslant x} \frac{1}{n^s} - \frac{x^{1-s}}{1-s} \right), \quad \text{if } 1 > s > 0.$$

You may prove that the above limit exists.

iii. $\sum_{n\leqslant x} n^s = \frac{x^s+1}{s+1} + O(x^s)$ for $s \geqslant 0$.

58. Let $f, g : [1, \infty) \to \mathbb{C}$. Prove that

$$g(x) = \sum_{n\leqslant x} f\left(\frac{x}{n}\right)$$

if and only if

$$f(x) = \sum_{n\leqslant x} \mu(n) g\left(\frac{x}{n}\right).$$

59. Derive from Problem No. 58 that

$$\sum_{n\leqslant x} \mu(n) \left[\frac{x}{n}\right] = 1.$$

60. Derive from Problem No. 58 and 57i. that

$$\sum_{n\leqslant x} \Lambda(n) \left[\frac{x}{n}\right] = x\log x - x + O(\log x).$$

61. Can you deduce from Problem 60 above that[4]

$$\sum_{p \leqslant x} \left[\frac{x}{p}\right] \log p = x \log x + O(x)$$

where the sum is over primes $p \leqslant x$?

Linear Recurrences

62. Find a formula for the nth term of the following order 2 recurrence sequences:

   i. $u_0 = 0, u_1 = 1$ and $u_n = 2u_{n-1} - u_{n-2}$ for $n \geqslant 2$.

   ii. $u_0 = 1, u_1 = 1$ and $u_n = 2u_{n-1} - u_{n-2}$ for $n \geqslant 2$.

   iii. $u_0 = 1, u_1 = 1$ and $u_n = 2u_{n-1} + 3u_{n-2}$ for $n \geqslant 2$.

63. Let a, b be fixed integers and let $U_n(a,b), V_n(a,b) \in \mathbb{C}(a,b)$[5] be defined by $U_0(a,b) = 0, U_1(a,b) = 1$ and $V_0(a,b) = 2, V_1(a,b) = a$. Suppose $1 - az - bz^2 = (1 - \lambda_1 z)(1 - \lambda_2 z)$ with $\lambda_1 \neq \lambda_2$. We shall sometimes write U_n, V_n in place of $U_n(a,b), V_n(a,b)$ if the reference to a, b is clear.

   i. Show that

$$U_n(a,b) = \frac{\lambda_1^n - \lambda_2^n}{\sqrt{D}};$$
$$V_n(a,b) = \lambda_1^n + \lambda_2^n$$

   where $D = a^2 + 4b$ denotes the discriminant of $1 - az - bz^2$.

   ii. Show that

$$\lambda_1^n = \frac{V_n + U_n\sqrt{D}}{2};$$
$$\lambda_2^n = \frac{V_n - U_n\sqrt{D}}{2}.$$

   iii. Show that

$$U_{2n} = U_n V_n, \qquad V_{2n} = V_n^2 - 2(-b)^n;$$
$$U_{n+1} = \frac{aU_n + V_n}{2}, \qquad V_{n+1} = DU_n + aV_n.$$

[4] Don't spend too much time on this. It won't come in exam!

[5] Recall that $\mathbb{C}(a,b)$ denotes the set of all complex sequences $(u_n)_{n \geqslant 0}$ satisfying $u_n = au_{n-1} + bu_{n-2}$ for all $n \geqslant 2$.

iv. Is it true that $\{(U_n)_{n\geqslant 0}, (V_n)_{n\geqslant 0}\}$ forms a basis of $\mathbb{C}(a,b)$?

Linear Diophantine Equations

64. Find all solutions of $10X + 7Y = 11$.

65. Prove that $aX + bY = c$ is solvable in integers if and only if $\gcd(a,b) = \gcd(a,b,c)$.

66. Find all *nonnegative* integral solutions (if any) of the linear diophantine equations:

    i. $3X + 7Y = 23$.

    ii. $2X + 5Y = 14$.

    iii. $5X + 7y = 23$.

    iv. $7X + 11Y = 75$.

67. Let $a > 0, b > 0$ be relatively prime and let $c \geqslant 0$. Show that there are nonnegative integers x, y such that $ax + by = c$ if $c > ab - a - b$. Are there nonnegative integers x, y such that $ax + by = ab - a - b$?

You can also find previous years' mid-sem, end-sem and back paper question papers here. Do give yourselves a good practice!