MTH 215- Assignment
IIT Kanpur year - 2020–21

We use notations same as in the course. We recall (a, b) denotes the gcd of a and b. $d(n) := \sigma_0(n) = \sum_{k|n} 1$, number of positive divisor of n.

1. Find greatest common divisor d of the numbers 1324 and 5490. Also, find number x and y such that
$$1324x + 5490y = d.$$

2. Prove that 4 does not divide $n^2 + 2$ for any integer n.

3. Prove that if n is odd, then 8 divides $n^2 - 1$. Prove that 6 divides $n^3 - n$.

4. Let n and k be two positive integers with $n \geqslant 2$. Prove that $(n-1)^2$ divides $n^k - 1$ if and only if $n - 1$ divides k.

5. Let a, b be two positive integers with $(a, b) = 1$. If $ab = c^2$, then prove that there exists integers x and y such that $a = x^2$ and $b = y^2$. More generally if $ab = c^n$, then $a = x^n$ and $b = y^n$.

6. Prove that $\text{ord}_p(a + b) \geqslant \min(\text{ord}_p a,\ \text{ord}_p b)$ with equality holds if $\text{ord}_p a \neq \text{ord}_p b$.

7. Determine all solutions in the integers of following Diophantine equations:

   (a) $18x + 5y = 48$.

   (b) $54x + 21y = 243$.

   (c) $158x - 57y = 7$.

   Also, determine all solutions in the positive integers in above equation.

8. Prove that $(n! + 1, (n + 1)! + 1) = 1$.

9. Let a and b are two positive integers with $b \geqslant 3$. Prove that $2^a + 1$ is not divisible by $2^b - 1$.

10. Let m and n are two positive integers with $m > n$. Let a be a positive integer. Prove that $a^{2^n} + 1$ is a divisor of $a^{2^m} - 1$. Also, prove that $(a^{2^m} + 1, a^{2^n} + 1) = 1$ if a is even and $(a^{2^m} + 1, a^{2^n} + 1) = 2$ if a is odd.

11. Prove that if $2^n + 1$ is a prime then n is a power of 2.

12. * If $a > 1$ prove that $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

13. Let $(a, b) = 1$. Then prove that there exists $x > 0, y > 0$ such that $ax - by = 1$.

14. Let $(a, b) = 1$ and $x^a = y^b$ for some integers x and y. Then prove that there exists an integer n such that $x = n^b$ and $y = n^a$.

15. prove that $\prod_{d|n} d = n^{d(n)/2}$.

16. prove that $\sum_{d|n} \mu^2(d) = 2^{\omega(n)}$.

17. prove that $\sum_{d|n} \mu(n/d)\tau(d) = 1$ and $\sum_{d|n} \mu(n/d)\sigma(d) = n$ for all n, where $\tau(n) = d(n)$ and $\sigma(n) = \sigma_1(n) = \sum_{d|n} d$.

18. Show that $\sum_{k|n} d(k)^3 = (\sum_{k|n} d(k))^2$ for all positive integer n.

19. Prove that $\sum_{d|n} \mu(d) \log^m d = 0$ if $m \geqslant 1$ and n has more than m distinct prime factors. (Hint: use induction on m).

20. Let f be an arithmetical function such that $f(n) > 0$ for all n. Let $a(n)$ be arithmetical function such that $a(n)$ is real for all n and $a(1) \neq 0$. Let $b(n)$ be the Dirichlet inverse of $a(n)$. Prove following product form of Möbius inversion formula

$$g(n) = \prod_{d|n} f(d)^{a(n/d)} \Longleftrightarrow f(n) = \prod_{d|n} g(d)^{a(n/d)}.$$

21. Let $f(x)$ be defined for all rational number x in the interval $[0, 1]$. Let $F(x)$ and $F_1(x)$ be defined by

$$F(n) = \sum_{k=1}^{n} f\left(\frac{k}{n}\right) \qquad \text{and} \qquad F_1(n) = \sum_{\substack{k=1 \\ (k,\ n)=1}}^{n} f\left(\frac{k}{n}\right).$$

Prove that

(i) $F_1 = F \star \mu$.

(ii) Using (i) (or some other way) prove that

$$\sum_{\substack{k=1 \\ (k,\ n)=1}}^{n} e\left(\frac{k}{n}\right) = \mu(n) \qquad \text{where } \ e(x) = e^{2\pi i x}.$$

22. Prove that $f(n) = \lfloor\sqrt{n}\rfloor - \lfloor\sqrt{n-1}\rfloor$ is a multiplicative function, but it is not completely multiplicative.

23. Let f be a multiplicative function. Examine whether $F(n) = \prod_{d|n} f(d)$ is multiplicative or not.

24. Let f be an arithmetical function (not necessarily multiplicative). Prove that there is a multiplicative arithmetical function g such that

$$\sum_{k=1}^{n} f((k, n)) = (f \star g)(n), \qquad \text{where } (k, n) = \gcd(k, n).$$

Taking $f(k) = (k,n)\mu((k,n))$ in above identity prove that

$$\sum_{k=1}^{n}(k,n)\mu((k,n)) = \mu(n).$$

25. Prove that Liouville function $\lambda(n)$ is given by formula

$$\lambda(n) = \sum_{d^2|n}\mu\left(\frac{n}{d^2}\right).$$

Chapter 3

Let $x \geqslant 2$ be a real number. Use Euler or Able summation formula (or by any new method) to prove that

26.

$$\sum_{n\leqslant x}\frac{\log n}{n} = \frac{1}{2}\log^2 x + A + O\left(\frac{\log x}{x}\right), \qquad \text{where } A \text{ is a constant.}$$

27.*

$$\sum_{n\leqslant x}\frac{1}{n\log n} = \log\log x + B + O\left(\frac{1}{x\log x}\right), \qquad \text{where } B \text{ is a constant.}$$

28.*

$$\sum_{n\leqslant x}\frac{d(n)}{n} = \frac{1}{2}\log^2 x + 2C\log x + O\left(1\right), \qquad \text{where } C \text{ is a constant.}$$

29. Let $\alpha > 0$, with $\alpha \neq 1$. Prove that

$$\sum_{n\leqslant x}\frac{d(n)}{n^\alpha} = \frac{x^{1-\alpha}\log x}{1-\alpha} + \zeta^2(\alpha) + O\left(x^{1-\alpha}\right).$$

30.*

$$\sum_{n\leqslant x}\phi(n) = \frac{1}{2}\sum_{n\leqslant x}\mu(n)\left\lfloor\frac{x}{n}\right\rfloor^2 + \frac{1}{2} = \frac{x^2}{2\zeta(2)} + O\left(x\log x\right).$$

31.

$$\sum_{n\leqslant x}\frac{\phi(n)}{n} = \sum_{n\leqslant x}\frac{\mu(n)}{n}\left\lfloor\frac{x}{n}\right\rfloor = \frac{x}{\zeta(2)} + O\left(\log x\right).$$

32.*

$$\sum_{n\leqslant x}\frac{\phi(n)}{n^2} = \frac{\log x}{\zeta(2)} + \frac{C}{\zeta(2)} - A + O\left(\frac{\log x}{x}\right), \qquad \text{where } A = \sum_{n=1}^{\infty}\frac{\mu(n)\log n}{n^2}.$$

33.* Assuming

$$\prod_p \left(1 - \frac{1}{p^2}\right)^{-1} = \zeta(2) = \frac{\pi^2}{6}, \qquad \text{prove that for } \; n \geqslant 2$$

$$\frac{\sigma(n)}{n} < \frac{n}{\phi(n)} < \frac{\pi^2}{6}\frac{\sigma(n)}{n}, \qquad \text{where } \sigma(n) = \sum_{d|n} d.$$

Also, prove that

$$\sum_{n \leqslant x} \frac{n}{\phi(n)} = O(x).$$

(Note: above estimate shows that $\phi(n)$ behaves like n on average).

34. For real $s > 0$ and integer $k \geqslant 1$ find an asymptotic formula for the partial sums

$$\sum_{\substack{n \leqslant x \\ (n,k)=1}} \frac{1}{n^s}$$

with an error term that tends to 0 as $x \to \infty$. Be sure to include the case $s = 1$.

35.* Let $\{x\}$ denotes the fractional part of x and $\lfloor x \rfloor$ denotes the integral part of x. What are the possible values of $\{x\} + \{-x\}$ and $\lfloor 2x \rfloor - 2\lfloor x \rfloor$. Prove that $\lfloor x \rfloor + \lfloor x + 1/2 \rfloor = \lfloor 2x \rfloor$.

36. Prove that $\lfloor 2x \rfloor + \lfloor 2y \rfloor \geqslant \lfloor x \rfloor + \lfloor y \rfloor + \lfloor x + y \rfloor$. Prove that

$$\sum_{k=0}^{n-1} \left\lfloor x + \frac{k}{n} \right\rfloor = \lfloor nx \rfloor \quad \text{and} \quad \sum_{k=0}^{n-1} f\left(x + \frac{k}{n}\right) = f(nx), \quad \text{where } f(x) = x - \lfloor x \rfloor - \frac{1}{2}.$$

With $f(x)$ as above, deduce that

$$\left| f\left(2^n x + \frac{1}{2}\right) \right| \leqslant 1 \quad \text{for all } m \geqslant 1 \text{ and all real } x.$$

37.* If n is a positive integer, prove that

$$\left\lfloor \sqrt{n} + \sqrt{n+1} \right\rfloor = \left\lfloor \sqrt{4n+2} \right\rfloor.$$

38. Determine all positive integer n such that $\lfloor \sqrt{n} \rfloor$ divides n.

39.* Prove that

$$\sum_{n \leqslant x} \lambda(n) \left\lfloor \frac{x}{n} \right\rfloor = \lfloor \sqrt{x} \rfloor.$$

(Hint: Use Theorem 2.13 and Corollary 3.1).

40. Prove that
$$\sum_{n\leqslant x}\left\lfloor\sqrt{\frac{x}{n}}\right\rfloor=\sum_{n\leqslant\sqrt{x}}\left\lfloor\frac{x}{n^2}\right\rfloor.$$
(Hint: Take $s(n)$ to be indicator function for squares and $S(x)=\sum_{n\leqslant x}s(n)$)

41.* Let S be a set of n integers (not necessarily distinct). Prove that some nonempty subset of S has a sum which is divisible by n. (Hint: use Pigeonhole principle).

42.* Find all positive integers n for which $n^{13}\equiv n(\text{mod } 1365)$. (Hint: Use Fermat little theorem)

43. Prove that $\phi(n)\equiv 2(\text{mod } 4)$ when $n=4$ and when $n=p^a$, where p is a prime with $p\equiv 3(\text{mod } 4)$.

44.* Find all x which simultaneously satisfy the system of congruences
$$x\equiv 1(\text{mod } 4),\quad x\equiv 2(\text{mod } 3),\quad x\equiv 2(\text{mod } 5)$$
.

⋆ ⋆ ⋆ ⋆ ⋆ ⋆ ⋆ ⋆

45. Prove that $\phi(n)\equiv 2(mod\ 4)$ when $n=4$ and $n=p^\alpha$, where p is prime $p\equiv 3(mod\ 4)$.

46. Find all n such that $\phi(n)\equiv 2(mod\ 4)$.

47. Let n be a positive integer which is not a square. Prove that for every integer a relatively prime to n there exist integers x and y satisfying
$$ax\equiv y(\mod n)\quad with\ 0<x<\sqrt{n}\ \ and\ \ 0<|y|<\sqrt{n}.$$

48. Let $p\equiv 1(mod\ 4)$ be a prime and $q=\frac{p-1}{2}$ and let $a=q!$. Prove that there exist positive integers x and y such that
$$a^2x^2\equiv y^2(\mod p)\quad with\ 0<x<\sqrt{p}\ \ and\ \ 0<y<\sqrt{p}.$$

49. For x and y in above question (question number 48) prove that $p=x^2+y^2$. This shows that every prime $p\equiv 1(mod 4)$ is sum of two square. Also, prove that no prime $p\equiv 3(mod\ 4)$ is sum of two square.

50. Using Theorem 5.32 of Apostol book (this has not been covered in class, please read the theorem first) prove the following:

Let n,a,d be given integers with $(a,d)=1$. Prove that there exists an integer m such that $m=a(mod\ d)$ and $(m,n)=1$. (Hint: Apply Theorem 5.32 with $k=nd$. Consider the set $S=\{a+td:t=1,2,\cdot(nd)/d\}$. By Theorem 5.32 there exists an $m\in S$ such that $(m,nd)=1$.

51. Let $(a|p)$ denotes the Legendre symbol $\left(\frac{a}{p}\right)$. Determine those odd primes p for which $(-3|p) = 1$ and those for which $(-3|p) = -1$.

52. Prove that 5 is a quadratic residue of an odd prime p if $p \equiv \pm 1(mod\ 10)$, and that 5 is a non-residue if $p \equiv \pm 3(mod\ 10)$.

53. Let $f(x)$ be a polynomial which takes integer values when x is an integer.

    (i) Let a, b be an integer with $(a, p) = 1$. Then

    $$\sum_{x(p)} \left(\frac{f(ax+b)}{p}\right) = \sum_{x(p)} \left(\frac{f(x}{p}\right) \quad and$$

    $$\sum_{x(p)} \left(\frac{af(x}{p}\right) = \left(\frac{a}{p}\right) \sum_{x(p)} \left(\frac{f(x}{p}\right) \quad for\ all\ a.$$

    (Hint: If x runs over all residue class mod p, then so does $ax+b$. And if $ax+b \equiv y(p)$, then $f(ax+b) \equiv f(y)(p)$).

    (ii) Let a, b be an integer with $(a, p) = 1$. Then

    $$\sum_{x(p)} \left(\frac{ax+b}{p}\right) = 0.$$

    (iii) Let $f(x) = x(ax+b)$, where $(ab, p) = 1$. Prove that

    $$\sum_{x=1}^{p-1} \left(\frac{f(x)}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{a+bx}{p}\right) = -\left(\frac{a}{p}\right).$$

    (Hind: if x runs through a reduced residue class mod p so does x', where $xx' \equiv 1(mod\ p)$. Also use that $(x|p)\ x'|p)$.

54. Let $\alpha, \beta \in \{1, -1\}$ (i.e., they takes values ± 1). Let $N(\alpha, \beta)$ denotes the number of integer x among $1, 2, \cdots p-2$ such that

    $$\left(\frac{x}{p}\right) = \alpha, \quad and \quad \left(\frac{x+1}{p}\right) = \beta.$$

    Prove that

    $$\begin{aligned} 4N(\alpha, \beta) &= \sum_{x=1}^{p-2} \left\{1 + \alpha \left(\frac{x}{p}\right)\right\} \left\{1 + \beta \left(\frac{x+1}{p}\right)\right\} \\ &= p - 2 - \beta - \alpha\beta - \alpha \left(\frac{-1}{p}\right). \end{aligned}$$

    (Hint: Let $0 < x < p-1$. Note that if $\alpha = (x|p)$, then $\{1 + \alpha(x|p)\} = 2$ and if $\alpha \neq (x|p)$, then $\{1 + \alpha(x|p)\} = 0$. Same scenario holds for β also. Hence

    $$\left\{1 + \alpha \left(\frac{x}{p}\right)\right\} \left\{1 + \beta \left(\frac{x+1}{p}\right)\right\} = \begin{cases} 4 & if\ \ \alpha = (x|p)\ and\ \ \beta = (x+1|p) \\ 0 & otherwise. \end{cases}$$

Hence total occurrence of parity get multiply by 4. For second part use part (iii) of 53 with $a = 1 = b$.

55. Use exercise 54 to prove that for every prime there exists integers x and y such that $x^2 + y^1 + 1 \equiv 0(mod\ p)$.

    Hint: (i) If $p \equiv 1(4)$, then -1 is a quadratic residue. Choose x such that $x^2 \equiv -1(mod\ p)$, and $y \equiv 0(p)$. We obtain that in this case $x^2 + y^1 + 1 \equiv 0(mod\ p)$. (ii) If $p \equiv 3(4)$, then -1 is a quadratic non-residue mod p. By previous exercise choose z such that $(z|p) = 1$ and $(z+1|p) = -1$. Hence $(-z-1|p) = 1$. Hence there exists x and y such that $x^2 \equiv z(modp)$ and $y^2 \equiv -z-1(modp)$.

56. Let p be an odd prime. Prove each of the following statements:

    (i) If $p \equiv 1(4)$, then

    $$\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right) = 0.$$

    (ii) If $p \equiv 1(4)$, then

    $$\sum_{\substack{r=1\\(r|p)=1}}^{p-1} r = \frac{p(p-1)}{4}.$$

    (iii) If $p \equiv 3(4)$, then

    $$\sum_{r=1}^{p-1} r^2\left(\frac{r}{p}\right) = p\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right).$$

    (Hint: if r runs through set $\{1, 2, \cdots p-1\}$ so does $p - r$. For part (ii), also use that -1 is quadratic residue mod p).

57. Prove that m is prime if and only if $\exp_m(a) = m - 1$ for some a.

58. Let g be a primitive root of an odd prime p. Prove that $-g$ is also a primitive root of p if $p \equiv 1(mod\ 4)$, but that $\exp_p(-g) = (p-1)/2$ if $p \equiv -1(mod\ 4)$.

59. Let p be an odd prime of the form $2^{2^k} + 1$. Prove that the set of primitive roots mod p is equal to the set of quadratic non-residues mod p. Use this result to prove that 7 is a primitive root of every such prime.

    (Hint: If n is an integer, then $2^n \equiv 1, 2, 4(mod\ 7)$. If g is a primitive root the $g^{(p-1)/2} \not\equiv 1(p)$. Hence by Euler's criterion i.e., $(a|p) \equiv a^{\frac{p-1}{2}}$ we obtain that $(g|p) = -1$. On the other hand if $(g|p) = -1$ then again by Euler's criterion $g^{(p-1)/2} \not\equiv 1(p)$. Since $\phi(p)$ is power of 2, every divisor d is also power of 2 and hence d divides $p - 1/2$. For second part of problem, use quadratic reciprocity.)

60. If p is an odd prime $\geqslant 5$, prove that the product P of all the primitive roots mod p is congruent to 1 mod p.

    (Hint: Let g be a primitive root. Then

$$P \equiv \prod_{\substack{k=1 \\ (k,p-1)=1}}^{p-1} g^k = g^\ell, \quad where \ \ \ell = \sum_{\substack{k=1 \\ (k,p-1)=1}}^{p-1} k = \frac{1}{2}(p-1)\phi(p-1).)$$

61. Prove that the sum of the primitive roots mod p is congruent to $\mu(p-1)$ mod p.

62. Assume that 7 is a primitive root for the prime $p = 71$. Find all primitive roots of 71 and also find a primitive root for p^2 and for $2p^2$.

    (Hint: Use Lemma 5.1 and Theorem 5.7).

63. Let p be and odd prime and $n > 1$. Let

$$S_p(n) = \sum_{k=1}^{p-1} k^n.$$

    Then $S_p(n) \equiv 0(p)$ if $n \not\equiv 0(p-1)$ and $S_p(n) \equiv -1$ if $n \equiv 0(p-1)$.

64. Determine the least positive solution (means a solution $x_1+\sqrt{N}y_1$ such that every other solution is power of it) for the following values of N in Pell's equation $x^2 - Ny^2 = 1$, for $N = 3, 7$. (Hint: use Theorem 6.2)

65. Show that if $N = n^2 - 1$ where n is a natural number then the least positive solution to $x^2 - Ny^2 = 1$ is given by $x = n$, $y = 1$. (Hint: use proof of Theorem 6.2)

66. If N is a square number then $x^2 - Ny^2 = 1$ has only trivial solutions.

67. A Dirichlet approximation $\frac{p}{q}$ to a real number α is call "D-approximation" if

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

    Prove that if two D-approximations both have denominator $q > 1$, then they are identical. And also, there are at most two D-approximations with the same denominator.

68. If α is a rational number then it has only finitely many D-approximation. (We have proved that irrationals have infinitely many).