PROBLEMS, SHEET 2, MP313, Semester 2, 1999.

1. Let $a|bc$, where $abc \neq 0$.

   (a) Prove that
   $$a|\gcd(a,b)\gcd(a,c).$$

   (b) Use induction to prove the generalization: Let $a|a_1\cdots a_n$. Then
   $$a|\gcd(a,a_1)\cdots\gcd(a,a_n).$$

2. Solve the congruence $256x \equiv 8 \pmod{337}$.

3. Let $m > 1, \gcd(a,m) = 1$. Prove that the congruence $ax \equiv b \pmod{m}$ has the solution
$$x \equiv ba^{\phi(m)-1} \pmod{m}.$$

4. Let $m, n \in \mathbb{N}$ and $d = \gcd(m,\ n)$. If $d \mid a - b$, prove that the system of congruences
$$x \equiv a \pmod{m} \qquad \text{and} \qquad x \equiv b \pmod{n}$$
has the solution
$$x \equiv ak\frac{n}{d} + bh\frac{m}{d} \pmod{l},$$
where $d = hm + kn$ and $l = \operatorname{lcm}(m,n)$.

5. Solve the system of congruences
$$x \equiv 1 \pmod{49}, \quad x \equiv 15 \pmod{21}, \quad x \equiv 12 \pmod{13}.$$

6. Solve the following systems of congruences by working in $\mathbb{Z}_{19}, \mathbb{Z}_{33}$, respectively:

   (a)
$$\begin{aligned} 3x + 3y &\equiv 1 \pmod{19} \\ 5x + 2y &\equiv 1 \pmod{19}. \end{aligned}$$

   (b)
$$\begin{aligned} 3x + 11y &\equiv 1 \pmod{33} \\ 11x + 3y &\equiv 1 \pmod{33}. \end{aligned}$$

   (Hint: In (b) use the identity $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = (ad - bc)I_2$.)

7. Let p be an odd prime and k a positive integer. Show that the congruence $x^2 \equiv 1 \pmod{p^k}$ has exactly two solutions mod p^k, namely $x \equiv \pm 1 \pmod{p^k}$.

8. Show that the congruence $x^2 \equiv 1 \pmod{2^k}$ has exactly four solutions mod 2^k, namely $x \equiv \pm 1$ or $x \equiv \pm(1 + 2^{k-1}) \pmod{2^k}$, when $k \geq 3$. Show that when $k = 1$ there is one solution and when $k = 2$ there are two solutions mod 2^k.

9. Calculate $d(270), \sigma(270), \phi(270), \mu(710)$.

10. If $\sigma(n) > 2n$ and p is a prime not dividing n, prove that $\sigma(pn) > 2pn$.

11. If $\phi(n)|(n-1)$, prove that n is squarefree.

12. Prove that
$$\sum_{d|n} |\mu(d)| = 2^{\omega(n)},$$
where $\omega(n)$ is the number of distinct prime factors of n.

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

14. (a) Let n be an odd positive integer.
Prove that $\sigma(n)$ is odd if and only if n is a perfect square.
Hint: Prove that if p is odd, then
$$1 + p + \ldots + p^m \text{ is } \begin{cases} \text{odd if } m \text{ is even,} \\ \text{even if } m \text{ is odd.} \end{cases}$$
(b) Let n be an even positive integer, $n = 2^a N$, where N is odd.
Prove that $\sigma(n)$ is odd if and only if N is a perfect square.

15. If $n = p^a q^b$, where p and q are distinct odd primes and $a \geq 1$, $b \geq 1$, prove that $\sigma(n) < 2n$.

16. If $n > 1$, prove that $\phi(n)|n \Leftrightarrow n = 2^a 3^b,\ a \geq 1, b \geq 0$.

17. Find all positive integers n satisfying
(a) $\phi(n) = 2$, (b) $\phi(n) = 4$, (c) $\phi(n) = 6$. .

18. If $n > 1$ is not a prime, prove that $\sigma(n) > n + \sqrt{n}$.

19. Von Mangoldt's function $\Lambda(n)$ is defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^m,\ p \text{ a prime, } m \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

(a) Prove that

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

(b) Deduce that

$$\Lambda(n) = -\sum_{d|n} \mu(d) \log d.$$

20. (a) By writing

$$\log n! = \sum_{m=1}^{n} \log m = \sum_{m=1}^{n} \sum_{d|m} \Lambda(d),$$

where $\Lambda(n)$ is Von Mangoldt's function, derive the formula

$$\alpha_p(n) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right], \tag{1}$$

where $p^{\alpha_p(n)}$ is the exact power of p which divides $n!$.

(b) If $n = a_0 + a_1 p + \cdots + a_r p^r$ is the expansion of n to base p, prove that

$$\alpha_p(n) = \frac{n - (a_0 + a_1 + \cdots + a_r)}{p - 1}.$$

(c) Prove that $\alpha_2(n) = n - \nu_2(n)$, where $\nu_2(n)$ is the number of ones in the binary expansion of n.

(d) Derive formula (1) directly, using a counting argument.

(e) Calculate the number of zero at the end of the decimal expansion of 100!

21. Prove that

$$\sum_{\substack{d=1 \\ \gcd(d,n)=1}}^{n} f(d) = \sum_{d|n} \mu(d) \sum_{t=1}^{n/d} f(td)$$

if $f : \mathbb{N} \to \mathbb{C}$ is a complex–valued function.

(Hint: Write the LHS as

$$\sum_{d=1}^{n} f(d) \sum_{D \mid \gcd(d,n)} \mu(D).)$$

22. If $n \in \mathbb{N}$, let

$$\psi_m(n) = \sum_{\substack{d=1 \\ \gcd(d,n)=1}}^{n} d^m.$$

(a) Prove that if $n > 1$,

$$\psi_1(n) = \frac{n}{2}\phi(n).$$

(b) Prove that

$$\psi_2(n) = \left(\frac{n^2}{3} + \frac{(-1)^t}{6} p_1 \dots p_t\right) \phi(n),$$

where $p_1, \dots, p_t$ are the distinct prime factors of n.

23. Prove that if $n \in \mathbb{N}$ and $n|(2^n - 1)$, then $n = 1$. [Hint: Suppose that there exists an $n \geq 2$ satisfying $n|(2^n - 1)$. Choose the least such n. Then use the identity

$$\gcd(2^n - 1,\, 2^{\phi(n)} - 1) = 2^{\gcd(n,\phi(n))} - 1$$

and the Euler–Fermat theorem.]

ASSIGNMENT 1

Please hand in Questions 1(a), 5, 6(a) and 13 by Friday 5pm, 13th August 1999.