Name: ID#: Serial #:

---

1. [10pts] (a) Let $a, b \in \mathbb{Z}$ and p be prime such that $(a, p^3) = p^2$, $(b, p^4) = p^3$. Find (ab, p^7) and $(a + b, p^7)$.

Solution. We have $p^2 \parallel a$ and $p^3 \parallel b$, hence $p^5 \parallel ab$ and $p^2 \parallel (a + b)$. This implies $(ab, p^7) = p^5$ and $(a + b, p^7) = p^2$.

(b) Let $m, n \in \mathbb{N}$, $m > 1$. Prove that if g is a primitive root mod m and $\gcd(n, \varphi(m)) = 1$, then g^n is a primitive root mod m.

Solution. We have $\text{ord}_m(g^n) = \dfrac{\varphi(m)}{(\varphi(m), n)} = \varphi(m)$, so g^n is a primitive root mod m.

---

2. [10pts] Let $f : \mathbb{N} \longrightarrow \mathbb{N}$ be defined by $f(n) = 2^r$ where $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ is a factorization of n into a product of distinct prime powers.

(a) Prove that f is multiplicative and that $\sum_{d|n} f(d) = \prod_{i=1}^{r} (1 + 2a_i)$

Solution. For each $n \in \mathbb{N}$, $f(n) = 2^{\omega(n)}$ where $\omega(n)$ is the number of distinct prime divisors of n. Hence $f(1) = 1$ and if $m, n \in \mathbb{N}$ and $(m, n) = 1$, then $\omega(mn) = \omega(m) + \omega(n)$ (since m and n have no prime divisor in common).

$$f(mn) = 2^{\omega(mn)} = 2^{\omega(m)+\omega(n)} = f(m) f(n).$$

So f is multiplicative and therefore so too is $\sum_{d|n} f(d)$. Let $F(n) = \sum_{d|n} f(d)$, where $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ is a factorization of n into a product of distinct prime powers. Note first that $F(1) = 1$ and for any prime power p^a,

$$F(p^a) = \sum_{d|p^a} f(d) = 1 + 2a.$$

Hence $F(n) = \prod_{i=1}^{r} F(p_i^{a_i}) = \prod_{i=1}^{r} (1 + 2a_i)$.

(b) Prove that $\sum_{d|n} \mu^2(d) = f(n)$, where μ is the Möbius function.

Solution. For each $n \in \mathbb{N}$, let $h(n) = \sum_{d|n} \mu^2(d)$. Clearly h is multiplicative (recall that μ is multiplicative), and for any prime power p^a,

$$h(p^a) = \sum_{d|p^a} \mu^2(d) = 2 = f(p^a).$$

Hence $\sum_{d|n} \mu^2(d) = f(n)$.

---

3. [15pts] Solve over $\mathbb{Z}$ each of the equations below.

(a) $x + 7y + 9z = 14$

Solution. If (x, y, z) is a solution over $\mathbb{Z}$ of the equation, then $x + 2y \equiv 0 \pmod 7$ and so $x = 7u - 2z$ for some $u \in \mathbb{Z}$. Hence $u + z = 2 - y$. We therefore obtain $x = 7u - 2v$, $y = 2 - u - v$, $z = v$, where

$u, v \in \mathbb{Z}$ (note of course that if $x = 7u - 2v,\ y = 2 - u - v,\ z = v$, then $x + 7y + 9z = 14$). [Note that there are infinitely many other equivalent parametric forms of the solution of this Diophantine equation.]

(b) $x^2 + y^2 = (x + y - 2)^2$

Solution. We can use the general parametric form of Pythagorean triples: $|x| = d\,(m^2 - n^2)$, $|y| = 2dmn$, $|x + y - 2| = d\,(m^2 + n^2)$ (where $m, n \in \mathbb{N}$, $m > n$ and d a nonnegative integer assuming, w.l.o.g., that y is even). However, expanding the RHS gives $2xy - 4x - 4y + 4 = 0$, i.e $(x - 2)(y - 2) = 2$. This means $x - 2 \in \{1, -1, 2, -2\}$ giving the 4 solutions $(3, 4), (1, 0), (4, 3), (0, 1)$.

(c) $x^2 + y^2 = 9z + 3$

Solution. If $x^2 + y^2 = 9z + 3$ is solvable over $\mathbb{Z}$, then $3|x^2 + y^2$ and so $x = 3a,\ y = 3b$ for some $a, b \in \mathbb{Z}$. We then get $9|\,(9z + 3)$ which is impossible. So the equation has no solution over $\mathbb{Z}$.

---

4. [10pts] (a) Let $m, n \in \mathbb{N}$.
(i) Find a polynomial equation with integer coefficients for which $\sqrt{m} - \sqrt{n}$ is a root and deduce that if $\sqrt{m} - \sqrt{n}$ is rational, then it must be an integer.

Solution. Let $a = \sqrt{m} - \sqrt{n}$. Then $a^2 = m + n - 2\sqrt{mn}$. Hence $2\sqrt{mn} = m + n - a^2$, i.e. $(m + n - a^2)^2 = 4mn$. So a is a root of the monic polynomial equation over $\mathbb{Z}$, $(m + n - x^2)^2 - 4mn = 0$. Therefore if $\sqrt{m} - \sqrt{n} \in \mathbb{Q}$, then $\sqrt{m} - \sqrt{n} \in \mathbb{Z}$.

(ii) Find all m in $\mathbb{N}$ for which $\sqrt{m} - \sqrt{2}$ is rational.

Solution. Let $b = \sqrt{m} - \sqrt{2}$ and assume $b \in \mathbb{Q}$. Then $\left(b + \sqrt{2}\right)^2 = m$, i.e. $2b\sqrt{2} = m - b^2 - 2 \in \mathbb{Q}$. Since $\sqrt{2} \notin \mathbb{Q}$, we deduce that $b = 0$. So the only m in $\mathbb{N}$ for which $\sqrt{m} - \sqrt{2} \in \mathbb{Q}$ is $m = 2$.

Another way. Let $\sqrt{m} - \sqrt{2} \in \mathbb{Q}$, then $\dfrac{m - 2}{\sqrt{m} + \sqrt{2}} \in \mathbb{Q}$. Assume for contradiction that $m - 2 \neq 0$, then $\sqrt{m} + \sqrt{2} \in \mathbb{Q}$ and so $2\sqrt{2} = \sqrt{m} + \sqrt{2} - \left(\sqrt{m} - \sqrt{2}\right) \in \mathbb{Q}$, which is impossible. So $m = 2$.

(b) Is π^3 algebraic? Justify.

Solution. If π^3 were algebraic, then there would be a nonzero polynomial $P(x)$ over $\mathbb{Z}$ such that $P(\pi^3) = 0$ and hence π would be a root of the polynomial equation $P(x^3) = 0$, which is impossible since π is not algebraic. Hence π^3 is not algebraic.

---

5. [15pts] (a) Let $b \equiv a^{11} \pmod{95}$ where $(a, 95) = 1$. Find a positive integer k such that

$$b^k \equiv a \pmod{95}$$

Solution. We need to find $k \in \mathbb{N}$ such that $11k \equiv 1 \pmod{\varphi(95)}$, i.e. $11k \equiv 1 \pmod{72}$. This means k is a positive solution of the system $11x \equiv 1 \pmod 8$, $11x \equiv 1 \pmod 9$, i.e. $x \equiv 3 \pmod 8$, $x \equiv 5 \pmod 9$. We get $x = 5 + 9t$ ($t \in \mathbb{Z}$) and $t \equiv 6 \pmod 8$, so that $x = 5 + 9(6 + 8r)$, where $r \in \mathbb{Z}$. We can therefore take $k = 59$.

(b) Determine whether 91 is a pseudoprime to the base 3.

Solution. We check whether $3^{90} \equiv 1 \pmod{91}$. We have $\varphi(91) = 72$, so $3^{90} \equiv 3^{18} \pmod{91}$. Now $3^{18} \equiv (3^3)^6 \equiv 1 \pmod 7$ and $3^{18} \equiv (3^3)^6 \equiv 1 \pmod{13}$. So $3^{18} \equiv 1 \pmod{91}$ and 91 is a pseudoprime to the base 3.

(c) Find a Carmichael number of the form $85p$ where p is prime.

Solution. Let $N = 85p$. For N to be a Carmichael number, 4, 16 and $p-1$ must divide $N-1$, i.e. $16|((16 \times 5p) + 5p - 1)$ and $(p-1)\,|\,(85(p-1) + 84)$. Hence $16|(p+3)$ and $(p-1)\,|84$. This means $p - 1 \geq 12$ and $p-1$ is an even divisor of 84, we can therefore take $p = 13$. [Note that another value of p is 29. We therefore get 2 Carmichael numbers of the form $85p$: 1105 and 2465.]

---

6. [10pts] (a) Let $a/b, a'/b', a''/b''$ be consecutive fractions in the same row of the Farey table. Show that $\dfrac{a'}{b'} = \dfrac{a+a''}{b+b''}$

Solution. We have $a'b - ab' = a''b' - a'b'' = 1$. So $a'(b+b'') = b'(a+a'')$.

(b) Without setting up the Farey table, find the fractions immediately to the right and to the left of $4/5$ in the 20^{th} row of the table.

Solution. Let a/b, c/d be the fractions immediately to the right and to the left (resp.) of $4/5$ in the 20^{th} row. Then $4b \equiv -1 \pmod 5$ and $b \in \{16, 17, 18, 19, 20\}$. Clearly $b = 16$ and then $a = \dfrac{1+4b}{5} = 13$, so $a/b = 13/16$.

Also, $4d \equiv 1 \pmod 5$ and $d \in \{16, 17, 18, 19, 20\}$ gives $d = 19$ and $c = 15$, so $c/d = 15/19$.