Name: ID#: Serial #:

---

1. [10pts] Let a, b be integers. Prove that

(a) If a is odd, then $(5a+4, 10a+4) = 1$.

Proof. $(5a+4, 10a+4) = (5a+4, 10a+4-2(5a+4)) = (5a+4, -4) = 1$ (since a odd implies $5a+4$ odd).

(b) If $(a, 4) = (b, 4) = 2$, then $(a+b, 4) = 4$.

Proof. Put $a = 2u$, $b = 2v$, then $(2u, 4) = 2$ implies $u = 2h+1$ for some $h \in \mathbb{Z}$, and similarly $v = 2k+1$ for some $k \in \mathbb{Z}$. Hence $(a+b, 4) = (4h+4k+4, 4) = 4$.

---

2. [10pts] (a) Find a positive integer n such that $n/3$ is a perfect square and $n/2$ is a perfect cube.

Solution. n is a multiple of 6, so put $n = 2^x 3^y$. We want x and $y-1$ to be even, $x-1$ and y to be multiples of 3. We can take $x = 4$, $y = 3$, i.e. $n = 2^4 3^3$.

Second way. Use the Fundamental Theorem of Arithmetic (this gives the form of all such n).

Third way. We have $n/3 = a^2$ and $n/2 = b^3$ for some $a, b \in \mathbb{N}$. Hence $n = 3a^2 = 2b^3$ so that $3|b$ and $2|a$ and there exist $c, d \in \mathbb{N}$ such that $b = 3c$ and $a = 2d$. This gives

$$n = 12d^2 = 2 \times 3^3 c^3$$

i.e. $2d^2 = 9c^3$ giving $d = 3e$, $c = 2f$ for some $e, f \in \mathbb{N}$. This in turn gives

$$e^2 = 4f^3.$$

So we can take $e = 2$, $f = 1$ and then $n = 3 \times 12^2$. (This argument, combined with the result in Part (b) also gives the form of all such n.)

(b) Let a, b positive integers such that $a^2 = b^3$. Prove there exists $c \in \mathbb{N}$ such that $a = c^3$ and $b = c^2$.

Proof. We can use the Fundamental Theorem of Arithmetic. A simpler proof is to say that $b^2 | b^3$ so $b^2 | a^2$, which gives $a = bc$ for some $c \in \mathbb{N}$. This means $b^2 c^2 = b^3$, so $b = c^2$ and then $a = c^3$.

---

3. [10pts] (a) Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$. Show that $a+1, a+2, \ldots, a+m$ is a complete residue system $\bmod m$.

Proof. The set $\{a+j : 1 \le j \le m\}$ contains exactly m elements and no two distinct elements of it are congruent $\bmod m$ since $a+i \equiv a+j (\bmod m)$, where $1 \le i \le j \le m$, implies $i = j$.

(b) Let $r_1, r_2, \ldots, r_k$ be a reduced residue system (RRS) $\bmod m$, where $m \in \mathbb{N}$. Suppose $(a, m) > 1$. Is $a+r_1, a+r_2, \ldots, a+r_k$ necessarily a RRS $\bmod m$? Justify your answer.

Solution. No: Take $m = 6$, $a = 3$. Then $1, 5$ is a reduced residue system mod 6 but $4, 8$ is not.

---

4. [10pts] (a) Prove that if p is an odd prime then $2(p-3)! \equiv -1 \pmod{p}$.

Proof. By Wilson's theorem, $(p-1)(p-2)(p-3)! \equiv -1 \pmod{p}$, so $2(p-3)! \equiv -1 \pmod{p}$.

(b) Prove that if a, b are coprime positive integers, then $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$.

Proof. By Euler-Fermat's theorem, $a^{\varphi(b)} \equiv 1 \pmod{b}$, so $a^{\varphi(b)} + b^{\varphi(a)} - 1 \equiv 0 \pmod{b}$, similarly $a^{\varphi(b)} + b^{\varphi(a)} - 1 \equiv 0 \pmod{a}$. Since $(a, b) = 1$, we get $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$.

---

5. [10pts] (a) Solve the congruence $x^2 + x + 1 \equiv 0 \pmod{49}$.

Solution. We can use trial and error to solve $x^2 + x + 1 \equiv 0 \pmod{7}$, however we can rewrite the congruence as $x^2 + x - 6 \equiv 0 \pmod{7}$, so that $(x-2)(x+3) \equiv 0 \pmod{7}$. This gives the solutions 2 and 4.

- Let $x = 2 + 7h$, where $h \in \mathbb{Z}$. Then

  $$(2+7h)^2 + (2+7h) + 1 \equiv 0 \pmod{49}$$

  gives $7(1+5h) \equiv 0 \pmod{49}$, i.e. $1 + 5h \equiv 0 \pmod{7}$. So $h \equiv 4 \pmod{7}$ and there is $k \in \mathbb{Z}$ such that $h = 4 + 7k$. Hence $x = 2 + 7(4+7k) \equiv 30 \pmod{49}$.

- Let $x = 4 + 7h$, where $h \in \mathbb{Z}$. Then

  $$(4+7h)^2 + (4+7h) + 1 \equiv 0 \pmod{49}$$

  gives $7(3+9h) \equiv 0 \pmod{49}$, i.e. $1 + 3h \equiv 0 \pmod{7}$. So $h \equiv 2 \pmod{7}$ and there is $k \in \mathbb{Z}$ such that $h = 2 + 7k$. Hence $x = 4 + 7(2+7k) \equiv 18 \pmod{49}$.

(b) Solve the system of congruences: $x \equiv 1 \pmod{3}$, $x \equiv 1 \pmod{5}$, $x \equiv 6 \pmod{10}$, $x \equiv 6 \pmod{11}$.

Solution. The system is equivalent to

$$x \equiv 1 \pmod{3}, \ x \equiv 6 \pmod{10}, \ x \equiv 6 \pmod{11}.$$

where $3, 10, 11$ are pairwise coprime, so that it has a unique solution $\bmod 330$.
Let $x = 6 + 11h$ (where $h \in \mathbb{Z}$), then $6 + 11h \equiv 6 \pmod{10}$ and so $h = 10k$ (where $k \in \mathbb{Z}$). We then get $x = 6 + 110k \equiv 1 \pmod{3}$, i.e. $k \equiv 2 \pmod{3}$. Let $k = 2 + 3l$ (where $l \in \mathbb{Z}$), so that $x = 6 + 110(2+3l)$. The solution of the system is therefore $226 \pmod{330}$.