Solutions to selected problems from homework 2

(1) Let p_1, p_2 be distinct primes. Using the Fundamental Theorem of Arithmetic prove that a natural number n is divisible by p_1p_2 if and only if n is divisible by p_1 and n is divisible by p_2.

Solution

It's obvious that of p_1p_2 divides n then both p_1 and p_2 divide n.

Suppose $p_1 \neq p_2$ are prime and $p_1|n$, $p_2|n$. Let $n = q_1 \cdot q_2 \cdot \ldots \cdot q_k$ be the prime factorization of n. Since $p_1|n$ we can write $n = p_1a$. We can also factor a into primes as $q = t_1 \cdot \ldots t_l$.

Then $n = q_1 \cdot q_2 \cdot \ldots \cdot q_k = p_1 \cdot a = p_1 \cdot t_1 \cdot \ldots t_l$.

By the Fundamental theorem of Arithmetic the factorization n is unique and therefore $p_1 = q_i$ for some i. Similarly, since $p_2|n$ we also have that $p_2 = q_j$ for some j. Since $p_1 \neq p_2$ we must have that $i \neq j$.

Therefore, $n = q_1 \cdot \ldots \cdot q_i \cdot \ldots \cdot q_j \cdot \ldots \cdot q_k = (p_1p_2) \cdot q_1 \cdot \ldots \cdot q_{i-1} \cdot q_{i+1} \cdot \ldots \cdot q_{j-1} \cdot q_{j+1} \cdot \ldots \cdot q_k$ and thus $p_1p_2|n$.

(2) (a) Find all possible values of $2^k \pmod 6$.
(b) Find all possible values of $k^2 \pmod 6$

Solution

(a) By trying the first few values of k we see that $2^1 = 2 \equiv 2 \pmod 6$. $2^2 = 4 \equiv 4 \pmod 6$, $2^3 = 8 \equiv 2 \pmod 6$, $2^4 = 16 \equiv 4 \pmod 6$. **Claim** $2^{2n} \equiv 4 \pmod 6$ and $2^{2n-1} \equiv 2 \pmod 6$ for any $n \geqslant 1$. Let us prove the second statement. The first is proved analogously. We will prove it by induction in n. When $n = 1$ we have $2^1 = 2 \equiv 2 \pmod 6$. Suppose $2^{2n-1} \equiv 2 \pmod 6$. Then $2^{2n+1} = 2^{2n-1} \cdot 4 \equiv 2 \cdot 4 \equiv 8 \equiv 2 \pmod 6$.

Answer: The possible values of $2^k \pmod 6$ for $k \geqslant 1$ are $2 \pmod 6$ and $4 \pmod 6$

(b) If $k \equiv 0 \pmod 6$ then $k^2 \equiv 0 \pmod 6$. If $k \equiv 1 \pmod 6$ then $k^2 \equiv 1^2 \equiv 1 \pmod 6$. If $k \equiv 2 \pmod 6$ then $k^2 \equiv 2^2 \equiv 4 \pmod 6$. If $k \equiv 3 \pmod 6$ then $k^2 \equiv 3^2 \equiv 3 \pmod 6$. If $k \equiv 4 \pmod 6$ then $k^2 \equiv 4^2 \equiv 4 \pmod 6$. If $k \equiv 5 \pmod 6$ then $k^2 \equiv 5^2 \equiv 1 \pmod 6$.

Answer: The possible values of $k^2 \pmod 6$ are $0 \pmod 6$, $1 \pmod 6$, $4 \pmod 6$, $3 \pmod 6$.

(3) Prove that if $m > 1$ is not prime then there exist integers a, b, c such that $c \not\equiv 0 \pmod m$, $ac \equiv bc \pmod m$ but $a \not\equiv b \pmod m$.

Solution

Let $m > 1$ be a composite number. Then it can be written as $m = a \cdot c$ where $1 < a, c < m$. Then $a \cdot c \equiv 0 \cdot c \equiv 0 \pmod m$ but $a \not\equiv 0 \pmod m$.

(4) #7 from the book. To find the last digit of 7^{22} we need to find $7^{22} \pmod{10}$.

We compute $7^2 = 49 \equiv -1 \pmod{10}$. Therefore $7^{22} = (7^2)^{11} \equiv (-1)^{11} \equiv -1 \equiv 9 \pmod{10}$.

Answer: The last digit of 7^{22} is 9.

(5) #24 from the book. We need to show that there are infinitely many primes of the form $4k + 3$. Suppose this is false and there are only finitely many such primes. Let $p_1, \ldots, p_n$ be all of them. We are given that $p_i \equiv 3 \pmod{4}$ for every i.

Let $N = 4(p_1 \cdot \ldots \cdot p_n) - 1$. Then $N \equiv -1 \equiv 3 \pmod{4}$. Consider the prime factorization of $N = q_1 \cdot \ldots q_l$. Note that since N is odd all q_j are odd. We claim that $p_i \neq q_j$ for any i, j. Suppose some of them are equal. Without loss of generality $p_1 = q_1$. Then $1 = 4(p_1 \cdot \ldots \cdot p_n) - q_1 \cdot \ldots \cdot q_l = 4(p_1 \cdot \ldots \cdot p_n) - p_1 \cdot q_2 \ldots \cdot q_l$ is divisible by p_1. this is impossible and hence $p_i \neq q_j$ for all i, j.

Next we claim that at least one q_j has the form $4k+3$. Every odd number is equal to either $1 \pmod{4}$ or $3 \pmod{4}$. If none of the q_j have the form $4k + 3$ then $q_j \equiv 1 \pmod{4}$ for every j. Therefore $N = q_1 \cdot \ldots \cdot q_l \equiv 1 \cdot \ldots \cdot 1 \equiv 1 \pmod{4}$. This is a contradiction since $N \equiv 3 \pmod{4}$.

Thus, for at least one j we must have $q_j \equiv 3 \pmod{4}$, i.e. $q_j = 4k + 3$ for some k. Since $q_j \neq p_i$ we have constructed a new prime number of the form $4k + 3$. This is a contradiction and hence there are infinitely many prime numbers of the form $4k + 3$. $\square$.