M328K: Homework 2

Katherine Ho

September 17, 2024

1. Let $\mathbb{G}$ denote the set of rational numbers that are greater than or equal to 1. Call an element $x \in \mathbb{G}$ a $\mathbb{G}$-*prime* if it cannot be factored as $x = yz$, where $y, z \in \mathbb{G}$, unless $y = 1$ or $z = 1$. Find all $\mathbb{G}$-primes. (Note: everything you do on homework should be assumed to be "with proof" unless otherwise specified.) Is it the case that every element of $\mathbb{G}$ can be factored as a product of $\mathbb{G}$-primes?

   Proof. Any rational number x can be expressed as the product of two rational numbers.

   $$x = \frac{p}{q} = \frac{p \cdot r}{1} \cdot \frac{1}{q \cdot r} \quad \text{where } p, q, r \in \mathbb{Z} \text{ and } q \neq 0$$

   This is true since any integer r can be multiplied by the first factor and divided by the second factor to create new rational numbers. r is then cancelled out during multiplication to yield the same x.
   However, the only number that cannot be factored as $x = yz$ unless $y = 1$ or $z = 1$ is 1.

   $$1 = \frac{p}{1} \cdot \frac{1}{q} \quad \text{where } p = 1 \text{ and } q = 1$$

   So, the only $\mathbb{G}$-prime is 1.

   $$\{x \mid x \text{ is a } \mathbb{G}\text{-prime}\} = \{1\}$$

   □

   Every element in $\mathbb{G}$ can be factored as a product of $\mathbb{G}$-primes since the only element is 1, which can be factored as a product of itself.

2. Prove each of the following assertions:

   (a) Any prime of the form $3n + 1$ is also of the form $6m + 1$.

   Proof. First, consider two cases.

   i. n is odd. ie. $n = 2a + 1$ for some $a \in \mathbb{Z}$

   $$\begin{aligned} 3n + 1 &= 3(2a + 1) + 1 \\ &= 6a + 4 \\ &= 2(3a + 2) \end{aligned}$$

   Thus we have $3n + 1$ is even.

ii. n is even. ie. $n = 2a$ for some $a \in \mathbb{Z}$

$$\begin{aligned} 3n + 1 &= 3(2a) + 1 \\ &= 2(3a) + 1 \end{aligned}$$

Thus we have $3n + 1$ is odd.

We know that 2 is the only even prime number since all even numbers greater than 2 are divisible by 2. Also, 2 cannot be expressed in the form $3n + 1$. Thus any prime of the form $3n + 1$ must be odd, where n is even. So, suppose $n = 2m$ for some $m \in \mathbb{Z}$.

$$3n + 1 = 3(2m) + 1 = 6m + 1$$

Thus any prime of the form $3n + 1$ is also of the form $6m + 1$. $\square$

(b) If p is a prime and $p \mid a^n$, then $p^n \mid a^n$.

Proof. Since $p \mid a^n$, $\exists a_k \in a^n$ such that $p \mid a_k$. Since $a_k = a$, we have

$$\begin{aligned} a &= px && \text{for some } x \in \mathbb{Z} \\ a^n &= p^n x^n && \text{By algebra} \end{aligned}$$

Thus $p^n | a^n$. $\square$

(c) If $p \neq 5$ is an odd prime, then either $p^2 - 1$ or $p^2 + 1$ is divisible by 10.

Proof. If $p \neq 5$ is odd, then p^2 is odd. Also, all odd prime numbers must end with $1, 3, 7$, or 9 so that they can't be divided by 2 or 5. Knowing this,

$$p \equiv 1, 3, 7, 9 \pmod{10}$$

This means that

$$p^2 \equiv 1, -1, -1, 1 \pmod{10}$$

Consider the following cases:

i. $p \equiv 1$ or $9 \pmod{10}$

$$\begin{aligned} p^2 &\equiv 1 \pmod{10} \\ p^2 - 1 &\equiv 0 \pmod{10} \\ 10 &\mid p^2 - 1 \end{aligned}$$

ii. $p \equiv 3$ or $7 \pmod{10}$

$$\begin{aligned} p^2 &\equiv -1 \pmod{10} \\ p^2 + 1 &\equiv 0 \pmod{10} \\ 10 &\mid p^2 + 1 \end{aligned}$$

Thus for any odd prime $p \neq 5$, either $p^2 - 1$ or $p^2 + 1$ is divisible by 10. $\square$

3. (a) Find all prime numbers that divide 50!. Prove that your list of primes is complete.

Proof. First, we have

$$50! = (50)(49)\dots(2)(1)$$

Each factor n in this product is an integer from 1 to 50. Each n can be written as a product of primes by the Fundamental Theorem of Arithmetic.

$$n = p_1^{a_1} p_2^{a_2} \dots p_{k_n}^{a_{k_n}} \qquad \text{for } 1 \leq n \leq 50$$

The prime factorization of 50! is the product of the prime factorizations of each n.

$$50! = \prod_{n=1}^{50} p_1^{a_1} p_2^{a_2} \dots p_{k_n}^{a_{k_n}}$$

Then, it can be said that for each integer from 1 to 50, none of their prime factorizations will contain a prime greater than 50. Thus the prime numbers that divide 50! are all of the prime numbers between 1 and 50.

$$\{p \mid p \text{ prime and } p \text{ divides } 50!\} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47\}$$

□

(b) Prove that $n > 4$ is composite, then $n \mid (n-1)!$

Proof. First, we know that

$$(n-1)! = (1)(2)\dots(n-1)$$

Since $n > 4$ is composite, we can say $n = ab$ for some $a, b \in \mathbb{Z}$ and $1 < a < b < n$. Also, a and b must be factors in $(n-1)!$.

$$(n-1)! = (1)(2)\dots(a-1)(a)(a+1)\dots(b-1)(b)(b+1)\dots(n-1)$$

Then, substitute $(a)(b) = n$.

$$(n-1)! = (1)(2)\dots(a-1)(a+1)\dots(b-1)(b+1)\dots(n-1)(n)$$

Thus $n \mid (n-1)!$. □

4. An integer is called *square-free* if it is not divisible by the square of any integer greater than 1. Prove the following:

(a) An integer $n > 1$ is square-free if and only if n can be factored into a product of distinct primes.

Proof by Contradiction. First, assume n is square-free. It can be represented as:

$$n = (p_1^{a_1})(p_2^{a_2})\dots(p_k^{a_k})$$

If some $a_i \geq 2$, then $p_i^2 \mid n$. However, this is a contradiction as n does not contain distinct primes. So, all a_i must be 1. Thus n is square-free iff n can be factored into a product of distinct primes. □

(b) Every integer $n > 1$ is the product of a square-free integer and a perfect square. (Hint: Use the canonical factorization of n.)

Proof. Every integer n can be expressed as a product of primes:

$$n = (p_1^{a_1})(p_2^{a_2})\dots(p_k^{a_k})$$

where each p_i is prime and each a_i is a positive integer. $a_i = 2q_i + r_i$, where $r_i = 0$ for even values of a_i and $r_i = 1$ for odd values of a_i. For odd values of a, we have

$$p_i^{a_i} = p_i^{2q_i+1} = p_i^{2q_i}p_i^1$$

Now, we can write n as the product of primes either to the power of 1 or $2q_i$. Then, by the commutative and associative properties n can be rearranged to be a product of two groups of primes.

$$n = ((p_i)\dots(p_j))((p_k^{2q_k})\dots(p_l^{2q_l}))$$

The first factor is the product of distinct primes. The second factor is a perfect square since it is the product of primes with even exponents. Thus every integer $n > 1$ is the product of a square-free integer and a perfect square.

$\square$

5. (a) Suppose $a \equiv b \pmod{m}$ and $n \mid m$. Prove that $a \equiv b \pmod{n}$.

Proof. First, we have $m = nx$ for some $x \in \mathbb{Z}$. By definition,

$$\begin{aligned} m &\mid (a-b) \\ nx &\mid (a-b) \\ a-b &= nx \cdot y \text{ for some } y \in \mathbb{Z} \\ a-b &= n(xy) \\ n &\mid (a-b) \end{aligned}$$

Thus $a \equiv b \pmod{n}$. $\square$

(b) Let p be prime. Show that if $x^2 \equiv 1 \pmod{p}$, then $x \equiv \pm 1 \pmod{p}$. Find a counterexample when p is not prime.

Proof. First, we have

$$\begin{aligned} p &\mid x^2 - 1 \\ p &\mid (x+1)(x-1) \end{aligned}$$

Given p is prime, $p \mid (x+1)$ or $p \mid (x-1)$. Now, we have

$$\begin{aligned} x - 1 \equiv 0 &\pmod{p} \quad \text{and} \quad x + 1 \equiv 0 \pmod{p} \\ x \equiv 1 &\pmod{p} \quad \text{and} \quad x \equiv -1 \pmod{p} \end{aligned}$$

Thus if $x^2 \equiv 1 \pmod{p}$, then $x \equiv \pm 1 \pmod{p}$ $\square$

A counterexample is $p = 8$.

$$3^2 \equiv 1 \pmod 8$$
$$3 \not\equiv 1 \pmod 8$$
$$3 \not\equiv -1 \pmod 8$$

(c) Suppose $a \equiv b \pmod m$. Prove that $\gcd(a, m) = \gcd(b, m)$.

Proof. First, we have $m \mid (a - b)$. Thus $a - b = mx$ for some $x \in \mathbb{Z}$.
Suppose the following:

i. $\gcd(a, m) = ax_1 + my_1 = z_1$ for some $x_1, y_1 \in \mathbb{Z}$

$$z_1 = ax_1 + my_1$$
$$z_1 = (mx + b)x_1 + my_1$$
$$z_1 = mxx_1 + bx_1 + my_1$$
$$z_1 = b(x_1) + m(xx_1 + y_1)$$

ii. $\gcd(b, m) = bx_2 + my_2 = z_2$ for some $x_2, y_2 \in \mathbb{Z}$

z_1 and z_2 are both linear combinations of b and m, so $z_1 = z_2$.
Thus $\gcd(a, m) = \gcd(b, m)$. $\square$