Homework 8

7.1 If \( n \) is not prime, then there are at least 2 prime factors \( p, q \) of \( n \) s.t. \( n \geq pq \).

Suppose that all prime factors of \( n \) are greater than \( \sqrt{n} \).

Then \( n > \sqrt{n} \cdot \sqrt{n} = n \), \( n > n \) is a contradiction.

Thus, \( n \) has a prime factor \( p < \sqrt{n} \).

7.2 \( n \neq 1 \), \( n \) and \( n+2 \) are relatively prime if \( n \) is odd.

1, 2, 15, 462, 227 are relatively prime.

and 15, 462, 1249 are relatively prime.

7.6 \( \gcd(157,7055,10872579) \)

\[ \gcd(10872579, 4697976) = \gcd(4697976, 1476627) \]

\[ = \gcd(1476627, 268095) = \gcd(268095, 136152) \]

\[ = \gcd(136152, 4209) = \gcd(4209, 1464) = \gcd(1464, 1281) \]

\[ = \gcd(1281, 183) = 183 \]

7.7 \( a \) and \( b \) are integers and \( m = \gcd(a, b) \). \( \frac{a}{m} \) and \( \frac{b}{m} \) are relatively prime integers.

If \( \frac{a}{m} \) and \( \frac{b}{m} \) are not relatively prime, \( \exists \ P > 1 \ s.t \ P \mid \frac{a}{m} \) and \( P \mid \frac{b}{m} \) (P62).

Thus, \( \frac{a}{m} \) and \( \frac{b}{m} \) are relatively prime.

8 \( a = \prod_{n=1}^{\infty} p_n^{n_n}, b = \prod_{n=1}^{\infty} p_n^{m_n} \), where \( \forall n \in \mathbb{N} \) and \( p_n \) is prime.

\( t_n = \min(n_n, m_n) \), then \( \gcd(a, b) = \prod_{n=1}^{\infty} p_n^{t_n} \).

First, \( \prod_{n=1}^{\infty} p_n^{t_n} \) is a and \( \prod_{n=1}^{\infty} p_n^{t_n} b \), we have \( \prod_{n=1}^{\infty} p_n^{t_n} \leq \gcd(a, b) \).

Then, Since \( \gcd(a) \) and \( \gcd(b) \), we have \( \gcd(ab) = \prod_{n=1}^{\infty} p_n^{t_n} \), where \( \forall n \in \mathbb{N} \).

Otherwise, \( \gcd(ab) = \prod_{n=1}^{\infty} p_n^{t_n} a \) or \( \prod_{n=1}^{\infty} p_n^{t_n} b \).

Then, \( \gcd(ab) \mid \prod_{n=1}^{\infty} p_n^{t_n} \) or \( \prod_{n=1}^{\infty} p_n^{t_n} = \gcd(ab) \mid \prod_{n=1}^{\infty} p_n^{t_n} \).

\( a \equiv 1 \mod{6} \), \( gcd(6, b) = \prod_{n=1}^{\infty} p_n^{t_n} \)
7.14 \( \mathbb{Z}_p = \{0, 1, 2, 3, \ldots, p-1\} \)

The roots of \( x^{p-1} \equiv 0 \) in \( \mathbb{Z}_p \) are the \( x \) s.t. \( x^{p-1} \equiv 1 \mod p \).

Thus they are \( 1, 2, 3, \ldots, p-1 \) by Fermat's Theorem.

2. \( p \) is an odd prime, thus \( \frac{p-1}{2} \) is an integer.

\( \mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\} \).

Since \( p \) is an odd prime, we have \( a^{p-1} \mod p = 1 \).

Since \( a^{p-1} = \alpha^{\frac{p-1}{2}}, \quad \alpha \in \mathbb{Z}_p \)

we have \( (a^{\frac{p-1}{2}} \mod p)(a^{\frac{p-1}{2}} \mod p) = a^{p-1} \mod p \equiv 1 \mod p \)

as a result, \( (a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) \mod p \equiv 0 \mod p \)

and \( \left[ a \right]^{\frac{p-1}{2}} = [1] \) or \( \left[ a \right]^{\frac{p-1}{2}} = [-1] = [p-1] \).

\( \frac{p-1}{2} \) of them satisfy (X) and \( \frac{p-1}{2} \) satisfy (XX).

Suppose \( \alpha \) satisfy (X) and \( \beta \) of them satisfy (XX), \( \alpha + \beta = p-1 \).

Let them \( \frac{\alpha + \beta + 1}{2} \).

Then, let \( k \) be an element of \( \mathbb{Z}_p \) elements \( \{k_1, k_2, \ldots, k_b\} \)

Let the \( k \) elements be \( \{k_1, k_2, \ldots, k_a\} \)

Then \( \{k_1, k_2, \ldots, k_b\} \) are different elements s.t. \( k_i^{\frac{p-1}{2}} \equiv -1 \mod p \)

So \( a \leq b \). Similarly, \( \{k_1, k_2, \ldots, k_b\} \) are \( b \) elements s.t. \( k_i^{\frac{p-1}{2}} \equiv 1 \mod p \).

So \( b \leq a \). \( \Rightarrow a = b = \frac{p-1}{2} \).

28.3 Without loss of generality, we can assume that \( a \in \{1, 2, \ldots, p-1\} \).

According to Fermat's little theorem, we have

\[ a^{p-1} \equiv 1 \mod p \]

This means \( (a, a^{p-2}) \equiv 1 \mod p \)

Thus, \( a^{p-2} \mod p \) is a reciprocal modulo \( p \) for \( a \).

28.4 (a) Integer Reciprocals (b) they are (c) according to (a) and (b),

\[ 1 \quad 1 \quad \frac{1}{3} \quad \frac{1}{4} \quad \frac{1}{5} \quad \frac{1}{6} \]

\[ 1, 2, \ldots, p-1 \]

\( (p-1)! \equiv 1 \cdot 2 \cdots (p-1) \equiv p-1 \mod p \)

\( \equiv -1 \mod p \)