Homework 8

7.1 If n is not prime, Then there are at least 2 prime factors of n (p_1, p_2) s.t. $n \geq p_1 p_2$

Suppose that all prime factors of n are greater than $\sqrt{n}$

Then $n \geq p_1 p_2 > (\sqrt{n} \cdot \sqrt{n}) = n$, $n > n$ is a contradiction.

Thus, n has a prime factor $p \leq \sqrt{n}$.

.3 $n \in \mathbb{N}$, n and $n+2$ are relatively prime if n is Odd.

.2 15,462,227 ~~are not relatively prime~~.

and 15,462,229 are ~~not~~ relatively prime.

7.6 $\gcd(15570555, 10872579)$

$= \gcd(10872579, 4697976) = \gcd(4697976, 1476627)$

$= \gcd(1476627, 268095) = \gcd(268095, 136152)$

$= \gcd(136152, 4209) = \gcd(4209, 1464) = \gcd(1464, 1281)$

$= \gcd(1281, 183) = 183$

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, $\exists\ p > 1$ $(p \in \mathbb{Z})$ s.t. $p \mid \frac{a}{m}$ and $p \mid \frac{b}{m}$.

As a result, $mp \mid a$ and $mp \mid b$, but $mp > m = \gcd(a,b)$ a contradiction.

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

8 $a = \prod_{n=1}^{N} p_n^{r_n}$, $b = \prod_{n=1}^{N} p_n^{s_n}$, where $p_n, r_n, s_n \in \mathbb{N}$ and p_n is prime

$t_n = \min(r_n, s_n)$, then $\gcd(a,b) = \prod_{n=1}^{N} p_n^{t_n}$

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

Then, since $\gcd \mid a$ and $\gcd \mid b$, we have $\gcd(a,b) = \prod_{n=1}^{N} p_n^{h_n}$, where $h_n \leq \min(r_n, s_n)$ otherwise, ~~gcd(a,b)~~ $\prod_{n=1}^{N} p_n^{h_n} \nmid a$ or $\prod_{n=1}^{N} p_n^{h_n} \nmid b$.

Then, $\gcd(a,b) \mid \prod_{n=1}^{N} p_n^{t_n}$ $\Rightarrow \gcd(a,b) \leq \prod_{n=1}^{N} p_n^{t_n}$. As a result, $\gcd(a,b) = \prod_{n=1}^{N} p_n^{t_n}$

7.14 $\mathbb{Z}_p = \{0,1,2,3,\dots,p-1\}$

roots of $x^{p-1}-[1]$ in $\mathbb{Z}_p$ are the x s.t. $x^{p-1} \equiv 1 \bmod p$.

Thus they are $1,2,3,\dots,p-1$ by Fermat's Theorem.

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

$\mathbb{Z}_p = \{0,1,2,\dots,p-1\}$.

Since $p \nmid a$, we have $a^{p-1} \bmod p = 1$.

Since $a^{p-1} = a^{\frac{p-1}{2}} \cdot a^{\frac{p-1}{2}}$

we have $(a^{\frac{p-1}{2}} \bmod p)(a^{\frac{p-1}{2}} \bmod p) \equiv a^{p-1} \bmod p \equiv 1 \bmod p$

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

and $\underbrace{[a]^{\frac{p-1}{2}} = [1]}_{(*)}$ or $\underbrace{[a]^{\frac{p-1}{2}} = [-1] = [p-1]}_{(**)}$.

$\frac{p-1}{2}$ of them satisfy (*) and $\frac{p-1}{2}$ satisfy (**)

Suppose a of them satisfy (*) and b of them satisfy (**), $a+b=p-1$.

Then, let k be an element of the b elements $\{k_1,k_2,\dots,k_b\}$

Let the a elements be $\{h_1,h_2,\dots,h_a\}$

Then $\{kh_1,kh_2,\dots,kh_a\}$ are a different elements s.t. $kh_i^{\frac{p-1}{2}} \equiv -1 \bmod p$

So $a \le b$. Similarly, $\{kk_1,kk_2,\dots,kk_b\}$ are b elements s.t. $kk_i^{\frac{p-1}{2}} \equiv 1 \bmod p$.

So $b \le a$. $\Rightarrow a=b=\frac{p-1}{2}$.

28.3 Without loss of generosity we can assume that $a \in \{1,2,\dots,p-1\}$

According to Fermat's little theorem, we have

$a^{p-1} \equiv 1 \bmod p$. This means $(a \cdot a^{p-2}) \equiv 1 \bmod p$

Thus, $a^{p-2} \bmod p$ is a reciprocal modulo p for a.

28.4. (a)

Integer	Reciprocal
1	1
2	4
3	5
4	2
5	3
6	6

(b) they are 1 and $p-1$

(c) according to (a) and (b),

$(p-1)! \equiv 1 \cdot 2 \cdots (p-1) \equiv p-1 \bmod p$

$\equiv -1 \bmod p$