VE203 Discrete Math
Spring 2022 — HW5 Solutions

April 16, 2022

Exercise 5.1

(i)

Since $a \equiv b(\bmod m)$, denote $a = r_1m + s, b = r_2m + s$ so that $a \equiv b \equiv s(\bmod m)(r, s \in \mathbb{Z})$. From $d \mid m$, we can represent m by $m = r_3d$. So $a = r_1r_3d + s, b = r_1r_3d + s.a \equiv s(\bmod d), b \equiv s(\bmod d)$, thus $a \equiv b(\bmod d)$.

(ii)

Similarly, denote $a = r_1m + s, b = r_2m + s$, so that $a \equiv b \equiv s(\bmod m)(r, s \in \mathbb{Z}).ac = r_1mc + sc$, $bc = r_2mc + sc.ac \equiv sc(\bmod mc), bc \equiv sc(\bmod mc)$, thus $ac \equiv bc(\bmod mc)$.

Exercise 5.2

(i)

If $ax \equiv ay(\bmod m) : m \left|(ax - ay) \Rightarrow \frac{m}{\gcd(a,m)}\right| \frac{a}{\gcd(a,m)}(x - y)$.

Since $\gcd\left(\frac{m}{\gcd(a,m)}, \frac{a}{\gcd(a,m)}\right) = 1, \frac{m}{\gcd(a,m)} \mid (x - y)$. So $x \equiv y \left(\bmod \frac{a}{\gcd(a,m)}\right)$

If $x \equiv y \left(\bmod \frac{a}{\gcd(a,m)}\right) : \frac{m}{\gcd(a,m)} |(x-y) \Rightarrow m| \gcd(a, m)\cdot(x-y)$. Since $\gcd(a, m)|a, m|a\cdot(x - y)$. So $ax \equiv ay(\bmod m)$.

So $ax \equiv ay(\bmod m) \Leftrightarrow x \equiv y \left(\bmod \frac{a}{\gcd(a,m)}\right)$.

(ii)

If $ax \equiv ay(\bmod m), m \mid (ax - ay)$. Since $\gcd(a, m) = 1, m \mid (x - y)$. So $x \equiv y(\bmod m)$.

Exercise 5.3

If $x \equiv y\,(\bmod m_i)$ for $i = 1, 2, \ldots, r : m_i \mid (x - y) \Rightarrow (x - y)$ is the common multiple of m_i.

So $\operatorname{lcm}(m_1, m_2, \ldots, m_r) \mid (x - y)$. So $x \equiv y\ (\bmod\ \operatorname{lcm}(m_1, m_2, \ldots, m_r))$.

If $x \equiv y\,(\bmod \operatorname{lcm}(m_1, m_2, \ldots, m_r))$:

Exercise 5.4

(i)

If $x^2 \equiv 1(\bmod p) : p\,|(x^2 - 1) \Rightarrow p|\,(x+1)(x-1)$. Since p is prime, either $p \mid (x+1)$ or $p \mid (x - 1)$. So $x \equiv \pm1(\bmod p)$.

If $x \equiv \pm1(\bmod p) : x^2 \equiv 1(\bmod p)$ by simply square both side.

So $x^2 \equiv 1(\bmod p) \Leftrightarrow x \equiv \pm1(\bmod p)$.

(ii)

For $p = 2, 1 \equiv -1(\bmod 2)$.

For $p \neq 2$, namely, p is odd:

The multiplicative group $X=(\mathbb{Z}/p\mathbb{Z})^{\times}=\{1,2,\ldots,p-1\}$ since p is prime and every integer less than p is coprime to p. As is shown in (i), the only solution of $x^2\equiv 1(\bmod p)$ for $x\in X$ is $x=1$ and $x=p-1$.

This is to say, x 's inverse does not equal to itself for $x\neq 1$ or $p-1$. Besides, there are even elements in $X\backslash\{1,p-1\}$. So we can always pair tow elements in $X\backslash\{1,p-1\}$ with their multiple equals 1 (mod p), i.e. $2\cdot 3\cdot\ldots\cdot(p-2)\equiv 1(\bmod p)$. Since $1\cdot(p-1)\equiv -1(\bmod p)$, so $(p-1)!\equiv -1(\bmod p)$.

(iii)

If $p\equiv 3(\bmod 4)$, $\frac{p-1}{2}$ is odd. For $x=1,2,\ldots,\frac{p-1}{2}, x\equiv -(p-x)(\bmod p)$. Since $(p-1)!\equiv 1\cdot(-1)\cdot 2\cdot(-2)\ldots\frac{p-1}{2}\cdot-\frac{p-1}{2}\equiv -1(\bmod p)$ and $\frac{p-1}{2}$ is odd, $-\left(\left(\frac{p-1}{2}\right)!\right)^2\equiv -1(\bmod p)$. According to (i), $\left(\frac{p-1}{2}\right)!\equiv \pm 1(\bmod p)$.

Exercise 5.5

$$561-1=280\cdot 2=56\cdot 10=35\cdot 16.\text{ So } a^{561-1}=\left(a^{3-1}\right)^{280}=\left(a^{11-1}\right)^{56}=\left(a^{17-1}\right)^{35}.$$

For $\gcd(a,3)=1, a^{560}\equiv 1(\bmod 3)$. For $\gcd(a,3)\neq 1$, i.e. $a\in 3\mathbb{Z}, 3\mid a$. Then, $3\mid a\left(a^{560}-1\right),\forall a\in\mathbb{Z}$ because either $3\mid a$ or $3\mid\left(a^{560}-1\right)$. Similar for 7 and 11. Therefore, $a^{561}\equiv a(\bmod 3), a^{561}\equiv a(\bmod 11)$, $a^{561}\equiv a(\bmod 17)$. So that $a^{561}-a$ is divisible by 3,11 and 17 and since they are pairwise relatively prime, $3\cdot 11\cdot 17\mid a^{561}-a$. i.e. $a^{561}\equiv a(\bmod 561)$ for all integer a.

Exercise 5.6

(i)

For $a\in Z$, because $a^q\equiv 1(\bmod p)$. we can get that $\gcd(a\cdot p)=1$. Hence. from Fermat's (Little) Theorem. we can get $a^{p-1}\equiv 1(\bmod p)$.

Therefore $a^{p-1}\equiv a^q\equiv 1(\bmod p)$. $\Leftrightarrow p\mid a^{\min\{p-1.q\}}\left(1-a^{\max(p-1.q)-\min\{p-1.q\}}\right)$. If a is identify element that $a\equiv 1(\bmod p)$. it's obviously true. If $p+a-1$. because $p+a$. hence. $a^{\max(p-1,q)-\min\{p-1,q\}}\equiv 1(\bmod p\ )$.

Therefore $|p-1-q|=nq(n\in z)$. $\Leftrightarrow p-1\equiv 0(\bmod q)\Leftrightarrow p\equiv 1(\bmod q)$. Hence. $a^q\equiv 1(\bmod p)\Rightarrow p\equiv 1(\bmod q) v a\equiv 1(\bmod p)$.

(ii)

Because 5|a. we can get that $a\equiv 0(\bmod 5)$

Hence. we can prove $5|a\wedge p|a^4+a^3+a^2+a+1\rightarrow P\equiv 1(\bmod 5)\Rightarrow$

$$a^5\equiv 1(\bmod p)\rightarrow p\equiv 1(\operatorname{mocl} 5)$$

Hence. we need to prove $5|a\wedge p|a^4+a^3+a^2+a+1\Rightarrow p\mid a^5-1$.

Because $a^5-1=(a-1)\left(a^4+a^3+a^2+a+1\right)$

Hence. $p\left|a^4+a^3+a^2+a+1\Rightarrow p\right|(a-1)\left(a^4+a^3+a^2+a+1\right)\Leftrightarrow p\mid a^5-1$. Therefore. we can get that $a^5\equiv 1(\bmod P)$ and $P\equiv 1(\bmod 5)$.

(iii)

Because $P\equiv 1(\bmod 5)\Leftrightarrow P=5n+1, n\in Z$ with $5|a\cap P|a^4+a^3+a^2+a+1$.

It's easy to find that $2\mid P$ and $P\in P$. therefore. $P=10n+1$. $n\in Z$.

Hence. for $\forall a(5\mid a)$. $\exists p=10n+1\ (p\mid a^4+a^3+a^2+a+1\wedge n\in Z\,.)$

Here we set $a=5m, m\in z$. and $k=a^4+a^3+a^2+a+1$.

For $k=5\left(125m^4+25m^3+5m^2+m\right)+1$, it's easy ts find that whether m is odd or m is even. $125m^4+25m^3+5m^2+m$ is even.

Hence. for $\forall k=10n+1(n\in Z), \exists p=10q+1(p\mid k\wedge q\in Z)$.

Here we assume the greatest prime $P_x=10n+1$.

For $S=2\times 3\times 5\times\cdots\times(10n+1)+1$. all primes from 2 to P_x are not the divisor.

and $S=(2\times 5)\times 3\times 7\times\cdots\times(10n+1)+1$ can be express as $S=10m+1$.

Therefore. there must exist a prime P with form $10n+1$ fits $P\mid S$. Hence. for every prime with form $10n+1$, there must exists a greater one with form $10n+1$. which means that there are infinitely many prines with form $10n+1$.

Exercise 5.7

Suppose $p\mid 2^{2^5}+1, p\le\sqrt{2^{2^5}+1}$. Hence, $2^{32}\equiv -1(\text{mod}p)$ and $2^{64}\equiv 1(\text{mod}p)$. By Fermat's theorem, $2^{p-1}\equiv 1(\text{mod}p)\Rightarrow p\equiv 1(\text{mod}64)$. By checking all $64k+1(k\in\mathbb{Z})$ in $0\le 64k+1\le 2^{16}$, we can find $F_5=641\times 6700417$.

Exercise 5.8

$2021=(11111100101)_2=2^{10}+2^9+2^8+2^7+2^6+2^5+2^2+2^0\cdot 2^{2^0}\equiv 2(\bmod 2021), 2^{2^2}\equiv 16$

$(\bmod 2021), 2^{2^5}\equiv 747(\bmod 2021), 2^{2^6}\equiv 213(\bmod 2021), 2^{2^7}\equiv 907(\bmod 2021), 2^{2^8}\equiv 102(\bmod 2021)$, $2^{2^9}\equiv 299(\bmod 2021), 2^{2^{10}}\equiv 477(\bmod 2021)\cdot 2^{2021}=2^{2^{10}}\cdot 2^{2^9}\cdot 2^{2^8}\cdot 2^{2^7}\cdot 2^{2^6}\cdot 2^{2^5}\cdot 2^{2^2}\cdot 2^{2^0}\equiv 477\cdot 299\cdot 102\cdot 907\cdot 213\cdot 747\cdot 16\cdot 2\equiv 388\cdot 907\cdot 213\cdot 747\cdot 4\equiv 1322(\bmod 2021)$. Since $2^{2021}\equiv 1322\not\equiv 2\ (\text{mod}2021), 2021$ is not a prime.

Exercise 5.9

To begin with, we deal with the first two linear congruence $x\equiv 2(\text{mod}4), x\equiv 5(\text{mod } 7)$. Solve $4u+7v=1$ and we easily get $u=2, v=-1. t_1=8\cdot 5-7\cdot 2\equiv 26(\text{mod}28)$. Then we deal with the last two linear congruence $x\equiv 0(\text{mod}11), x\equiv 8(\text{mod}15)$. Solve $11m+15n=1$ and we get $m=-4, n=3$. $t_2=-44\cdot 8+45\cdot 0=-352\equiv -22(\text{mod}165)$. Finally we deal with $x\equiv 26(\text{mod}28), x\equiv -22(\text{mod } 165)$. Solve $28p+165q=1$ and we get $p=-53, q=9$. $\quad t=-1484\cdot(-22)+1485\cdot 26=71258\equiv 1958\ (\text{mod}4620)$. Thus the final solution $x=1958$.

Exercise 5.10

(i)

$$6x\equiv 2\cdot 3x\equiv 2\cdot 0\equiv 0(\text{mod}3)$$

Therefore $6x\equiv 2(\text{mod}5)$ does not have solutions.

(ii)

$$6x\equiv x+5x\equiv x+0\equiv x(\text{mod}5)$$

Since there are infinitely many x that satisfies $x\equiv 2(\text{mod}5)$, such as $5k+2, (k\in\mathbb{Z}, 6x\equiv 2(\text{mod}5)$ has infinitely many solutions.

Exercise 5.11

i) $e(233) = 233^{95} \pmod{323}$

Since $95 = 2^6 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0$

$233^{95} = 233^{64} \times 235^{16} \times 233^8 \times 233^4 \times 233^2 \times 233^1$

$233^1 \equiv 233 \pmod{323}$

$233^2 \equiv 25 \pmod{323}$

$233^4 \equiv 25^2 \equiv 302 \pmod{323}$

$233^8 \equiv 302^2 \equiv 118 \pmod{323}$

$233^{16} \equiv 118^2 \equiv 35 \pmod{323}$

$233^{32} \equiv 35^2 \equiv 256 \pmod{323}$

$233^{64} \equiv 256^2 \equiv 290 \pmod{323}$

$\Rightarrow 233^{95} \equiv 290 \times 35 \times 118 \times 302 \times 25 \times 233 \equiv 180 \pmod{323}$

ii) $D = E^{-1} \pmod{\varphi(n)}$

$d(y) = y^D = x^{ED} \equiv x \bmod n$

$d(y) = y^{191} \bmod 323$

iii) $d(180) = 180^{191} \bmod 323$

Since $191 = 2^7 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0$

$180^{191} = 18^{128} \times 180^{32} \times 18^{16} \times 180^8 \times 18^4 \times 18^2 \times 180^1$

$180^1 \equiv 180 \pmod{323}$

$180^2 \equiv 100 \pmod{323}$

$180^4 \equiv 100^2 \equiv 310 \pmod{323}$

$180^8 \equiv 310^2 \equiv 169 \pmod{323}$

$180^{16} \equiv 169^2 \equiv 137 \pmod{323}$

$180^{32} \equiv 137^2 \equiv 35 \pmod{323}$

$180^{64} \equiv 35^2 \equiv 256 \pmod{323}$

$180^{128} \equiv 256^2 \equiv 290 \pmod{323}$

$\Rightarrow 180^{191} \equiv 290 \times 35 \times 137 \times 169 \times 310 \times 100 \times 180 \equiv 233 \pmod{323}$