Exercise 9

Discrete Mathematics

December 10, 2020

Theorem (Euler, Fermat):

$$\gcd(a, m) = 1 \implies a^{\varphi(m)} \equiv 1 \mod m \tag{1}$$

Theorem (Fermat):

$$p \in \mathbb{P}, p \nmid a \implies a^{p-1} \equiv 1 \mod p \tag{2}$$

Theorem (Chinese remainder theorem): Suppose $m_1, \ldots, m_k \in \mathbb{N}_+$ pairwisely co-prime and $a_1, \ldots, a_k \in \mathbb{Z}$ then the solution of the system

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\cdots \\ x &\equiv a_k \mod m_k \end{aligned}$$

of congruences is explicitly given by

$$x \equiv \sum_{i=1}^{k} \frac{m}{m_i} b_i a_i \mod m \tag{3}$$

where $m = m_1 \cdot m_2 \ldots m_k$ and $b_i = \left(\frac{m}{m_i}\right)^{-1} \mod m_i$.

Exercise 81

https://math.stackexchange.com/a/34223

Accepted this way

What we want is to calculate $2^{1000} \mod 100$.

As $\varphi(25) = 20$ we get by Euler's theorem 1 that $2^{20} \equiv 1 \mod 25$ and therefore $2^{1000} \equiv \left(2^{20}\right)^{50} \equiv 1^{50} \equiv 1 \mod 25$. Additionally, as $2^2 \equiv 0 \mod 4$ every multiple of

2^2 is also congruent 0 mod 4, especially $2^{1000} \equiv 0 \mod 4$. This gives us the system of congruences

$$x \equiv 1 \mod 25$$
$$x \equiv 0 \mod 4.$$

Note that

1. 25 and 4 are coprime
2. $b_1 = \left(\frac{25\cdot 4}{25}\right)^{-1} \mod 25$ is solved with $4z \equiv 1 \mod 25$. So $z = b_1 = 19$.

Therefore, by the chinese remainder theorem 3 we get

$$x \equiv \frac{25\cdot 4}{25} 19 \cdot 1 + \frac{25 \cdot 4}{4} b_2 \cdot 0 \mod 25 \cdot 4$$
$$x \equiv 76 \mod 100$$

So the last two digits of 2^{1000} are 76.

Exercise 82

16 might be wrong, should be 13 maybe? Was too fast for me We know

$$\gcd(a, m) = 1 \implies a^{\varphi(m)} \equiv 1 \mod m$$

$$\varphi(m) = m \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_r}\right) \quad \text{for } m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

Assume $\gcd(a, b) = 1$. Then holds $a^{\varphi(b)} \equiv 1 \mod b$. By laws of exponents we get

$$a \cdot \underbrace{a^{\varphi(b)-1}}_{c} \equiv 1 \mod b.$$

For the example, take in mind that $55 = 5 \cdot 11$ and $34 = 2 \cdot 17$. We see that $\gcd(55, 34) = 1$. Therefore,

$$55^{\varphi(34)} \equiv 1 \mod 34$$

and

$$\varphi(34) = 34 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{17}\right) = 16$$

It follows

$$55^{16} \equiv 55 \cdot 55^{15} \equiv 1 \mod 34$$

Exercise 83

(a) *Presented was taking Bézouts theorem to the power of 4 and bringing it into the required form a²x*aby*b²z=1 for some integers xyz because something like that was on Stackexchange, but that did not really work out*

We know Euclid's lemma

$$p \in \mathbb{P} \land p \mid xy \implies p \mid x \lor p \mid y \tag{4}$$

Proof by contraposition. Assume there is $d > 1$ such that $\gcd(a^2, ab, b^2)$. We know that

$$\gcd(a^2, ab, b^2) = \prod_{p \in \mathbb{P}} p^{\min\left(\nu_p(a^2), \nu_p(ab), \nu_p(b^2)\right)}$$

Therefore, at there exists at least one $q \in \mathbb{P}$ with $\nu_q(a^2) \geq 1$ or $\nu_q(ab) \geq 1$ or $\nu_q(b^2) \geq 1$. Then q is a factor of the $\gcd(a^2, ab, b^2)$. By the definition of gcd, it then divides all of them. By Euclid's lemma 4 holds $q \mid a^2 \implies q \mid a$ and $q \mid b^2 \implies q \mid b$ This means that q is a common divisor of a and b. Additionally, q is prime, it must hold $q > 1$. It follows $\gcd(a, b) > 1$ which concludes the proof by contraposition.

(b) Consider $a = 7^3, b = 7^2$. Then $a^2 = 7^6$ and $b^3 = 7^6$. $7^6 \mid 7^6$ is true. However, the only x for which $7^3 x = 7^2$ holds is $x = 1/7$ which is not an integer. Hence, by definition $7^3 \nmid 7^2$ and $a \nmid b$. This disproves the statement.

Exercise 84

Tutor argued that if you take an element x to some power, then you certainly get another element. and that x^a and x^a will never be the same. Something like the the mapping stuff. There was also a nice proof using Bézouts Theorem first and then doing a case distinction.

- https://math.stackexchange.com/q/709249
- https://math.stackexchange.com/q/2842399
- https://math.stackexchange.com/q/1491103
- https://math.stackexchange.com/q/3631921
- https://mathoverflow.net/q/53677
- link

Copy & paste some definitions into Google: Some are from nice freely available PDFs (like definition of discrete logarithm)

Assume $p \in \mathbb{P}$ satisfies $\gcd(a, p-1) = 1$. Let $b \in \mathbb{Z}$ be arbitrary. We take the discrete logarithm wrt a primitive root g:

$$\begin{aligned} x^a &\equiv b \mod p \\ ind_g\left(x^a\right) &\equiv ind_g\left(b\right) \mod p-1 \\ a \cdot ind_g\left(x\right) &\equiv ind_g\left(b\right) \mod p-1 \end{aligned}$$

Theorem from lecture:

$$ax \equiv b \mod m \text{ solvable} \iff \gcd(a, m) \mid b \tag{5}$$

The assumption $\gcd(a, p-1) = 1$ and the fact $1 \mid ind_g(b)$ show that $x^a \equiv b \mod p$ admits a solution.

Background

- Every field is a ring. Every ring is a group.
- The set of (congruence classes of) integers modulo n with the operations of addition and multiplication is a ring. It is denoted $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/(n)$. wiki This is our $\mathbb{Z}_m$.
- For prime p holds $\mathbb{Z}/p\mathbb{Z}$ is a finite field (Galois field), denoted $\mathbb{F}_p$ wiki
- The discrete logarithm over prime fields is defined as follows: Let $p > 2$ be a prime and x be a primitive root of p. We know that every $b \in \{1, 2, \ldots, p-1\}$ can be expressed as a power of $x \mod p$. That is,

  $$x^a \equiv b \mod p$$

  for a unique a modulo $p-1$. Then a is called the discrete logarithm or index of b with respect ot the base x modulo p.
- We see that the $\{1, 2, \ldots, p-1\}$ of b are exactly the elements of $\mathbb{Z}_p^*$. a modulo $p-1$ means, that means $a \in \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{p-2}\} = \mathbb{Z}_{p-1}$ (no star!).

Example: 2 is a generator for $p = 5$: $< \bar{2} >= \mathbb{Z}_5^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

- $2^1 \equiv 2 \mod 5$
- $2^2 \equiv 4 \mod 5$
- $2^3 \equiv 3 \mod 5$
- $2^4 \equiv 1 \mod 5$

For the discrete logarithm we look for the exponents of the previous enumeration, by using the knowledge that $\mathbb{Z}_5^*$ is cyclic. For example, we know that $\bar{3}$ is expressed as $(\bar{2})^a$ for some a. Note that we generated 1 by 2^4, but by our previous definition the discrete logarithm of $\bar{1}$ with respect to the base $\bar{2}$ modulo 5 is $\bar{0}$. Note $\bar{0} \in \mathbb{Z}_{p-1}$ and $\bar{4} \notin \mathbb{Z}_{p-1}$. More generally, we do not necessarily know which element of $\mathbb{Z}_5^*$ is its generator, but we know that there is some x with some a such that $x^a = b$.

We know from the lecture: $\mathbb{Z}_p^*$ is cyclic. This means there is a generator g. It follows that each element of $\mathbb{Z}_p^*$ can be expressed as g^a for some a. g is a primitive root $\mod m$ if g is a generator of $\mathbb{Z}_m^*$.

Different expressions for x,b

$\mathbb{Z}_p^*$ is cyclic as $p \in \mathbb{P}$. Then there is a generator x of $\mathbb{Z}_p^*$. We know that each element can be expressed with the generator, so let $b = x^s$ for some s. We try to find a number $1 \leq e \leq p-1$ such that $(x^e)^a = x^s$. That means we want is $x^{ea} \equiv x^s \mod p$. We can apply the discrete logarithm (index) as follows

$$\begin{aligned} x^{ea} &\equiv x^s \mod p \\ ind_x\left(x^{ea}\right) &\equiv ind_x\left(x^s\right) \mod p-1 \\ ea &\equiv s \mod p-1 \end{aligned}$$

We know from the lecture that such an equivalence is solvable if and only if $\gcd(a, p-1) \mid s$. Our assumption was that $\gcd(a, p-1) = 1$ and $1 \mid s$.

Mapping

As $p \in \mathbb{P}$ $\gcd(a, p)$ can only be 1 or multiples of p for any $a \in \mathbb{Z}$.

Case 1 $b \equiv 0 \mod p$. Then $b \equiv 0^a \mod p$. Hence, $x^a \equiv b \mod p$ admits a solution.

Case 2 $b \not\equiv 0 \mod p$. Then $\gcd(b, p) = 1$. Since $\gcd(a, p-1) = 1$ there exist $u, v \in \mathbb{N}$ such that $au = 1+(p-1)v$. Then $(b^u)^a = b^{au} = b^{1+(p-1)v} = b(b^{p-1})^v \equiv b \mod p$. This is because the Euler-Fermat theorem says $\gcd(b, p) = 1 \implies b^{\varphi(p)} \equiv 1 \mod p$ and it holds $\forall p \in \mathbb{P} : \varphi(p) = p-1$

Therefore, the mapping $x \rightarrowtail x^a$ on Z_p^* is surjective. As both domain and codomain of the map are equal, the mapping is even bijective. This means there is exactly one solution of $x^a \equiv b \mod p$. Hence, $x^a \equiv b \mod p$ admits a solution.

Subset

$\{1^a, 2^a, \ldots (p-1)^a, p^a\}$ is a subset of $\mathbb{Z}_p^*$ for any a. For example

- $1^3 \equiv 1 \mod 5$
- $2^3 \equiv 3 \mod 5$

- $3^3 \equiv 2 \mod 5$
- $4^3 \equiv 4 \mod 5$
- $5^3 \equiv 0 \mod 5$

and

- $1^4 \equiv 1 \mod 5$
- $2^4 \equiv 1 \mod 5$
- $3^4 \equiv 1 \mod 5$
- $4^4 \equiv 1 \mod 5$
- $5^4 \equiv 0 \mod 5$

Case 1 $b \equiv 0 \mod p$. It holds $p^a \equiv 0 \mod p$, so x^a has a solution. This means $x^a \equiv b \mod p$ admits a solution.

Case 2 $b \not\equiv 0 \mod p$. If $x^a \equiv b \mod p$ has no solution (second example enumeration), then $x^a = x^y$ for some distinct elements of $\mathbb{Z}_p$. Then holds $z^a = 1$ for $z = x \cdot y^{-1}$. By applying the discrete logarithm on both sides we get

$$\begin{aligned} z^a &\equiv 1 \mod p \\ ind_g(z^a) &\equiv ind_g(1) \mod p-1 \\ a \cdot ind_g(z) &\equiv 0 \mod p-1 \end{aligned}$$

We can apply the definition of congruence to get $p-1 \mid a \cdot ind_g(z)$. As p is prime, $p-1$ is even. Then $2 \mid p-1 \mid a \cdot ind_g(z)$. By assumption $\gcd(a, p-1) = 1$. But t$2 > 1$. Contradiction.

Exercise 85

712 is correct according to tutor

We first have to solve each congruence equations to get only x in front. Note that

$$\begin{aligned} 14x &\equiv 2 \mod 22 \\ 14x &= 2 + 22k \\ 7x &= 1 + 11k \\ 7x &\equiv 1 \mod 11 \end{aligned}$$

and similar for the other equations. So we seek such k that x is an integer.

$$\begin{aligned} 5x \equiv 8 \mod 32 &\implies x \equiv 8 \mod 32 \\ 14x \equiv 2 \mod 22 &\implies x \equiv 8 \mod 11 \\ 9x \equiv 3 \mod 15 &\implies x \equiv 2 \mod 5 \end{aligned}$$

Therefore, by 3 x is explicitly given by

$$
\begin{aligned}
x &= \frac{32 \cdot 11 \cdot 5}{32} \cdot b_1 \cdot 8 + \frac{32 \cdot 11 \cdot 5}{11} \cdot b_2 \cdot 8 + \frac{32 \cdot 11 \cdot 5}{5} \cdot b_3 \cdot 2 \mod 32 \cdot 11 \cdot 5 \\
&= 55 \cdot 7 \cdot 8 + 160 \cdot 2 \cdot 8 + 352 \cdot 3 \cdot 2 \equiv 7752 \equiv 712 \mod 1760
\end{aligned}
$$

where

$$
\begin{aligned}
b_1 &= \left(\frac{32 \cdot 11 \cdot 5}{32}\right)^{-1} \mod 32 \implies 55z \equiv 1 \mod 32 \implies z \equiv b_1 \equiv 7 \mod 32 \\
b_2 &= \left(\frac{32 \cdot 11 \cdot 5}{11}\right)^{-1} \mod 11 \implies 160z \equiv 1 \mod 11 \implies z \equiv b_2 \equiv 2 \mod 11 \\
b_3 &= \left(\frac{32 \cdot 11 \cdot 5}{5}\right)^{-1} \mod 5 \implies 352z \equiv 1 \mod 5 \implies z \equiv b_3 \equiv 3 \mod 5
\end{aligned}
$$

Exercise 86

By prime factorization we get $172872 = 2^3 \cdot 3^2 \cdot 7^4$. We know from the lecture

$$\lambda\left(\prod_{i=1}^{r} p_i^{e_i}\right) = lcm\left(\lambda\left(p_1^{e_1}\right), \ldots, \lambda\left(p_r^{e_r}\right)\right) \tag{6}$$

$$\lambda\left(p^k\right) = \varphi\left(p^k\right) \qquad \text{for } p \in \mathbb{P}, p > 2 \tag{7}$$

$$\lambda\left(2^k\right) = 2^{k-2} \qquad \text{for } k \geq 3 \tag{8}$$

$$\varphi\left(p^k\right) = p^k \cdot \left(1 - \frac{1}{p}\right) \tag{9}$$

$$\varphi(m) = m \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \cdots \cdot \left(1 - \frac{1}{p_r}\right) \qquad \text{for } m = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} \tag{10}$$

Therefore

$$
\begin{aligned}
\lambda(172872) &= \lambda\left(2^3 \cdot 3^2 \cdot 7^4\right) \\
&= lcm\left(\lambda\left(2^3\right), \lambda\left(3^2\right), \lambda\left(7^4\right)\right) \\
&= lcm\left(2^{3-2}, \varphi\left(3^2\right), \varphi\left(7^4\right)\right) \\
&= lcm\left(2^{3-2}, 3^2 \cdot \left(1 - \frac{1}{3}\right), 7^4 \cdot \left(1 - \frac{1}{7}\right)\right) \\
&= lcm(2, 6, 2058) \\
&= 2058
\end{aligned}
$$

as $2058 = 2 \cdot 3 \cdot 7^3$ and $6 = 2 \cdot 3$. And

$$\begin{aligned}\varphi(172872) &= 172872 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{7}\right) \\ &= 49392\end{aligned}$$

Exercise 87

Presented proof was similar, just more verbose https://math.stackexchange.com/a/2569172

We know from the lecture

$$\varphi(m) = m \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_r}\right) \qquad \text{for } m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

Let $d = \gcd(m, n)$. It follows

$$\frac{\varphi(mn)}{mn} = \prod_{p|mn} (1 - \frac{1}{p}) = \frac{\prod_{p|m}(1 - \frac{1}{p}) \prod_{p|n}(1 - \frac{1}{p})}{\prod_{p|d}(1 - \frac{1}{p})} = \frac{\frac{\varphi(m)}{m} \frac{\varphi(n)}{n}}{\frac{\varphi(d)}{d}}$$

Hence,

$$\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$$

Example:

$$\frac{\varphi(12 \cdot 20)}{12 \cdot 20} = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = \frac{\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)}{\left(1 - \frac{1}{2}\right)}$$

Exercise 88

Presented proof looked relatively similar and was generally accepted. Tutor mentioned that for $p = 2$ we might have to make a special case. We have to show that

$$\begin{aligned}\frac{lcm\,(b_1, b_2, \dots, b_k)}{lcm\,(a_1, a_2, \dots, a_k)} &= \frac{\prod_{p \in \mathbb{P}} p^{\max(\nu_p(b_1), \nu_p(b_2), \dots, \nu_p(b_k))}}{\prod_{p \in \mathbb{P}} p^{\max(\nu_p(a_1), \nu_p(a_2), \dots, \nu_p(a_k))}} \\ &= \prod_{p \in \mathbb{P}} p^{\max(\nu_p(b_1), \nu_p(b_2), \dots, \nu_p(b_k)) - \max(\nu_p(a_1), \nu_p(a_2), \dots, \nu_p(a_k))}\end{aligned}$$

is an integer. From $a_i \mid b_i$ for $1 \leq i \leq k$ follows $\forall p \in \mathbb{P} : \nu_p(a_i) \leq \nu_p(b_i)$. As the relation holds componentwise, it holds also for the maximum $\max(\nu_p(a_1), \nu_p(a_2), \dots, \nu_p(a_k)) \leq \max(\nu_p(b_1), \nu_p(b_2), \dots, \nu_p(b_k))$. Consequently

$$\max(\nu_p(b_1), \nu_p(b_2), \dots, \nu_p(b_k)) - \max(\nu_p(a_1), \nu_p(a_2), \dots, \nu_p(a_k)) = \nu_p'$$

exists and $\nu'_p \geq 0$. Therefore

$$\frac{lcm\left(b_1, b_2, \ldots, b_k\right)}{lcm\left(a_1, a_2, \ldots, a_k\right)} = \prod_{p \in \mathbb{P}} p^{\nu'_p}$$

is an integer. Therefore we get the result

$$a_i \mid b_i \text{ for } 1 \leq i \leq k \implies lcm\left(a_1, a_2, \ldots, a_k\right) \mid lcm\left(b_1, b_2, \ldots, b_k\right) \tag{11}$$

Example:

$$b_1 = 9, b_2 = 12, b_3 = 10 \qquad b_1 = 3^2, b_2 = 2^2 \cdot 3, b_3 = 2 \cdot 5$$
$$a_1 = 3, a_2 = 4, a_3 = 5 \qquad a_1 = 3, a_2 = 2^2, a_3 = 5$$
$$lcm\left(b_1, b_2, b_3\right) = 2^{\max(0,2,1)} \cdot 3^{\max(2,1,0)} \cdot 5^{\max(0,0,1)}$$
$$lcm\left(a_1, a_2, a_3\right) = 2^{\max(0,2,0)} \cdot 3^{\max(1,0,0)} \cdot 5^{\max(0,0,1)}$$

We know

$$\lambda\left(\prod_{i=1}^{r} p_i^{e_i}\right) = lcm\left(\lambda\left(p_1^{e_1}\right), \ldots, \lambda\left(p_r^{e_r}\right)\right) \tag{12}$$

$$\lambda\left(p^k\right) = p^{k-1}(p-1) \text{ for } p \in \mathbb{P}, p > 2 \tag{13}$$

$$m \mid n \Leftrightarrow \forall p \in \mathbb{P} : \nu_p(m) \leq \nu_p(n) \tag{14}$$

Assume $m \mid n$. Then $\forall p \in \mathbb{P} : \nu_p(m) \leq \nu_p(n)$. From this follows

$$\forall p \in \mathbb{P} : p^{\nu_p(m)} \mid p^{\nu_p(n)}. \tag{15}$$

Take in mind that $p_i^{e_i} = p^{\nu_p(m)}$ and $e_i = \nu_p(m)$ for some $p \in \mathbb{P}$.
We also know that

$$\lambda(m) = lcm\left((p_1-1)p_1^{e_1-1}, (p_2-1)p_2^{e_2-1}, \ldots, (p_r-1)p^{e_r-1}\right)$$
$$\lambda(n) = lcm\left((p_1-1)p_1^{f_1-1}, (p_2-1)p_2^{f_2-1}, \ldots, (p_s-1)p^{f_r-1}\right)$$

Consequently, $(p_i-1)p_1^{f_i-1} \mid (p_i-1)p_1^{e_i-1}$ for $1 \leq i \leq r$.
By our previous result 11 we get $\lambda(m) \mid \lambda(n)$.

Exercise 89

Calculate $3233/p$ for $p \in \mathbb{P}$ until you get an integer as result. We find $53 \cdot 61 = 3233$. With prime factorization we calculate $v = lcm(52, 60) = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 13 = 780$. We now look for a solution for $d \cdot 49 \equiv 1 \mod 780$. We then try different x in $\frac{1+780x}{49}$ until we get an integer as result. At $x = 37$ we get $d = 589$.

Exercise 90

After some discussion during the presentation it seemed that really taking CO, MP, UT, ER together is asked for. Using WolframAlpha was OK.

$$\begin{aligned}
CO = 0315 &\implies 315^{49} \mod 3233 = 2701 \\
MP = 1316 &\implies 1316^{49} \mod 3233 = 2593 \\
UT = 2120 &\implies 2120^{49} \mod 3233 = 371 \\
ER = 0518 &\implies 518^{49} \mod 3233 = 1002
\end{aligned}$$