Homework 8

Aleck Zhao

April 20, 2017

1. Let $p, x, n \in \mathbb{Z}$ with p prime and $n > 0$.

   (a) Prove that if $p \mid x^n$ then $p \mid x$.

   Proof. By the FTA, x must factor uniquely into a product of primes. Suppose

   $$x = p_1^{e_1} \cdots p_k^{e_k}$$

   for $p_1, \cdots p_k$ distinct primes, and $1 \le e_1, \cdots, e_k \in \mathbb{Z}$. Then we have

   $$x^n = (p_1^{e_1} \cdots p_k^{e_k})^n = p_1^{ne_1} \cdots p_k^{ne_k}$$

   If $p \mid x^n$, then since p is a prime, it must be one of the p_i's in the factorization. But then since this p_i appears in the factorization of x, it follows that $p \mid x$. $\square$

   (b) Show that the statement need not be true if p is not prime.

   Proof. If $p = 4, x = 6, n = 2$, then $4 \mid 6^2 = 36$ but $4 \nmid 6$. $\square$

2. Use the Fundamental Theorem of Arithmetic (FTA) to show that $\log_{21} 143$ is irrational.

   Proof. Suppose $\log_{21} 143$ was rational. Then $\log_{21} 143 = p/q$ for some $p, q \in \mathbb{Z}, q \neq 0$, and

   $$\begin{aligned} q \log_{21} 143 &= p \\ \implies 21^{q \log_{21} 143} &= 21^p \\ \implies 143 \cdot 21^q &= 21^p \\ \implies 11 \cdot 13 \cdot 3^q \cdot 7^q &= 3^p \cdot 7^p \end{aligned}$$

   By the FTA, since 11 and 13 are primes and appear on the LHS, they must appear in the factorization on the RHS, but since they don't, this is a contradiction. Thus $\log_{21} 143$ is irrational. $\square$

3. Let $a, b, c, n \in \mathbb{Z}$ with $n > 1$.

   (a) Prove that if $\gcd(c, n) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

   Proof. Since $\gcd(c, n) = 1$, the inverse of c exists in modulo n. Thus, we have

   $$\begin{aligned} ac &\equiv bc \pmod{n} \\ \implies ac(c^{-1}) &\equiv bc(c^{-1}) \pmod{n} \\ \implies a &\equiv b \pmod{n} \end{aligned}$$

   $\square$

   (b) Show that the statement in part (a) need not be true if c and n are not relatively prime.

   Proof. If $c = 6$ and $n = 4$, then $1 \cdot 6 \equiv 3 \cdot 6 \pmod{4}$ but $1 \not\equiv 3 \pmod{4}$. $\square$

4. Let $a, b, c, d, n \in \mathbb{Z}$ with $n > 1$. Prove that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then

   (a) $a + c \equiv b + d \pmod{n}$

   Proof. If $a \equiv b \pmod{n}$ then $n \mid (a - b)$ and similarly $n \mid (c - d)$. Thus, $n \mid [(a - b) + (c - d)] = (a + c - b - d)$, so $a + c \equiv b + d \pmod{n}$. □

   (b) $ac \equiv bd \pmod{n}$

   Proof. If $a \equiv b \pmod{n}$ then $ac \equiv bc \pmod{n}$. Similarly, if $c \equiv d \pmod{n}$ then $bc \equiv bd \pmod{n}$. Since $\equiv$ is transitive, it follows that $ac \equiv bd \pmod{n}$. □

5. In this problem we will use direct proof to prove the following statement: Let $a, p \in \mathbb{Z}$. If p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$.

   (a) We are given that $a, p \in \mathbb{Z}, p$ is prime, and $p \nmid a$. Explain why this mean $a \neq 0$.

   Answer. If $a = 0$, then $p \mid a$ since 0 is divisible by nonzero integer, which is a contradiction.

   (b) Let $S = \{a, 2a, 3, \cdots, (p-1)a\}$. Let $x, y \in S$ with $x \neq y$. Prove $x \not\equiv y \pmod{p}$.

   Proof. Suppose $x \equiv y \pmod{p}$, then $p \mid (x - y)$. Since $x, y \in S$, we have $x = ma$ and $y = na$ for $1 \leq m, n \leq p - 1$. Thus $x - y = ma - na = a(m - n)$, so $p \mid a(m - n)$. Since $p \nmid a$, we must have $p \mid (m - n)$, but this is only possible if $m - n = 0 \implies m = n$, which contradicts the fact that $x \neq y$. Thus $x \not\equiv y \pmod{p}$. □

   (c) Let $T = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ and let $f : S \to T$ be given by the rule $f(s) = s \mod p$. Prove f is a bijection.

   Proof. To show f is well defined, suppose $ma, na \in S$ and $ma = na$. Then

$$\begin{aligned} ma &= q_1 p + r_1 \\ na &= q_2 p + r_2 \end{aligned}$$

   but since this representation is unique and $ma = na$, it follows that $r_1 = r_2$ so

$$f(ma) = ma \mod p = na \mod p = f(na)$$

   Now, suppose for $ma, na \in S$, we have $r = f(ma) = f(na)$. Then we have

$$\begin{aligned} ma &= q_1 p + r \\ na &= q_2 p + r \\ \implies ma - na &= (q_1 p + r) - (q_2 p + r) = q_1 p - q_2 p = (q_1 - q_2)p \end{aligned}$$

   Thus, $p \mid (ma - na)$ so $ma \equiv na \pmod{p}$, but from part (b), this is impossible if $ma \neq na$, so we must have $ma = na$, and thus f is injective.
   The distinct values in T are $1, \cdots, p - 1$, and since $|S| = p - 1 = |T|$ and f is injective, it must also be surjective. Thus, f is a bijection. □

   (d) Explain why

$$\prod_{s \in S} s \equiv \prod_{t \in T} t \pmod{p}$$

   Answer. Since the elements of S and the elements of T are in bijection under f, for every $s \in S$, there is a corresponding $t \in T$ such that $f(s) = s \mod p = t$ Thus, taking the product of all of these pairs, we obtain the required relation.

(e) Explain why p and $(p-1)!$ are relatively prime.

Answer. Since p is a prime, it is not divisible by anything less than it other than 1. Thus, none of $2, \cdots, p-1$ share any common prime factors with p since otherwise p would have a factor less than p, which is impossible since p is a prime. Thus, the product $2 \cdots (p-1) = (p-1)!$ doesn't share any common prime factors with p, so they are relatively prime.

(f) Based on your work in parts (d) and (e), conclude that $a^{p-1} \equiv 1 \pmod{p}$.

Solution. From (d), we have

$$\prod_{s \in S} s = \prod_{i=1}^{p-1} ia = a \cdot 2a \cdots (p-1)a = (p-1)! \cdot a^{p-1}$$

$$\prod_{t \in T} t \pmod{p} = \prod_{t=1}^{p-1} t \pmod{p} \equiv (p-1)! \pmod{p}$$

$$\implies (p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod{p}$$

Since $\gcd[p, (p-1)!] = 1$, the inverse of $(p-1)!$ exists in modulo p, so multiplying by that inverse on both sides, we get $a^{p-1} \equiv 1 \pmod{p}$, as desired. □

6. In a transposition cipher we use permutations to help encode text. First we select a positive integer m. Let $M = \{\, x \in \mathbb{N} \mid 1 \leq x \leq m \,\}$. Next, we create a permutation $f : M \to M$. we then take the text message and split its letters into blocks of size m. We encode the block $b_1 b_2 \cdots b_m$ as $c_1 c_2 \cdots c_m$ where $c_i = b_{f(i)}$.

(a) Suppose $m = 4$ and $f(1) = 3, f(2) = 1, f(3) = 4, f(4) = 2$. Use the transposition cipher to encode PIRATE ATTACK.

Solution. The blocks of size $m = 4$ are PIRA, TEAT, TACK. Thus, we have

$$f : \begin{cases} 1 & \mapsto 3 \\ 2 & \mapsto 1 \\ 3 & \mapsto 4 \\ 4 & \mapsto 2 \end{cases} \implies \begin{cases} PIRA & \mapsto IAPR \\ TEAT & \mapsto ETTA \\ TACK & \mapsto AKTC \end{cases}$$

so the encoded message is IAPRETTAAKTC. □

(b) We decrypt an encoded transposition cipher message by using f^{-1}. For the function provided in part (a), what is f^{-1}?

Solution. $f^{-1} \circ f = \mathrm{id}$ so we must have

$$f^{-1} : \begin{cases} 1 & \mapsto 2 \\ 2 & \mapsto 4 \\ 3 & \mapsto 1 \\ 4 & \mapsto 3 \end{cases}$$

□

(c) Using the decryption function you obtained in part (b), decode SWUETRAEOEHS.

Solution. The blocks of size $m = 4$ are SWUE, TRAE, OEHS. Thus, we have

$$f^{-1} : \begin{cases} 1 & \mapsto 2 \\ 2 & \mapsto 4 \\ 3 & \mapsto 1 \\ 4 & \mapsto 3 \end{cases} \implies \begin{cases} SWUE & \mapsto USEW \\ TRAE & \mapsto ATER \\ OEHS & \mapsto HOSE \end{cases}$$

so the decoded message is USE WATER HOSE. □

7. Suppose $n = 713 = 23 \times 31$.

   (a) Let $e = 43$. Bob's encryption function is $E(M) = M^e \mod n$. what is his decryption function?

   Solution. This is RSA encryption. We have $\varphi(713) = (23-1)(31-1) = 660$. Now, suppose the decryption function is $D(N) = N^d \mod n$. Then we must have $de \equiv 1 \implies d \equiv e^{-1} \pmod{660}$. Thus, we must find e^{-1} in modulo 660, which exists because $\gcd(43, 660) = 1$. We have

$$\begin{aligned}
660 &= 15 \cdot 43 + 15 \\
43 &= 2 \cdot 15 + 13 \\
15 &= 1 \cdot 13 + 2 \\
13 &= 6 \cdot 2 + 1 \\
\implies 1 &= 13 - 6 \cdot 2 \\
&= 13 - 6 \cdot (15 - 1 \cdot 13) = 7 \cdot 13 - 6 \cdot 15 \\
&= 7 \cdot (43 - 2 \cdot 15) - 6 \cdot 15 = 7 \cdot 43 - 20 \cdot 15 \\
&= 7 \cdot 43 - 20 \cdot (660 - 15 \cdot 43) = 307 \cdot 43 - 20 \cdot 660
\end{aligned}$$

   Thus, $43^{-1} = 307$, so $d = 307$, and thus $D(N) = N^{307} \mod 713$ is the decryption function. $\square$

   (b) Encrypt the word I using Bob's encryption function.

   Solution. I is equivalent to 9, so we have $E(9) = 9^{43} \mod 713$. We have

$$\begin{aligned}
9^2 &= 9 \cdot 9 = 81 \mod 731 \\
9^4 &= 9^2 \cdot 9^2 = 81 \cdot 81 = 144 \mod 713 \\
9^8 &= 9^4 \cdot 9^4 \equiv 144 \otimes 144 = 59 \mod 713 \\
9^{16} &= 9^8 \cdot 9^8 \equiv 59 \otimes 59 = 629 \mod 713 \\
9^{32} &= 9^{16} \cdot 9^{16} \equiv 629 \otimes 629 = 639 \mod 713 \\
9^{11} &= 9 \cdot 9^2 \cdot 9^8 \equiv 9 \otimes 81 \otimes 59 = 231 \mod 731 \\
9^{43} &= 9^{32} \cdot 9^{11} \equiv 639 \cdot 231 = 18 \mod 713
\end{aligned}$$

   Thus, $E(9) = 18 \to R$. $\square$

   (c) Let $d = 43$. Sue's decryption function is $D(N) = N^d \mod n$. What is Sue's encryption function?

   Solution. If the encryption function is $E(M) = M^e \mod 713$, then we have $D(E(M)) = M^{ed} \mod 713 = M$. If $d = 43$, then by switching the roles of d and e in part (a), we have $e = 307$, so the encryption function is $E(M) = M^{307} \mod 713$. $\square$