Assignment#3 CS201 Fall 2023

Ben Chen(12212231)

November 4, 2023

PROBLEM 1. Show that if a, b and c are integers such that $ac \mid bc$, where $a \neq 0$ and $c \neq 0$, then $a \mid b$.

SOLUTION. Proof

$$\begin{aligned} ac \mid bc &\equiv \exists k,\ bc = k \cdot ac \\ &\equiv b = k \cdot a && \text{since } c \neq 0 \\ &\equiv a \Big| b && \text{Divisibility} \end{aligned}$$

PROBLEM 2. Evaluate the following quantities

SOLUTION. **a)** $-2023 = -62 \times 33 + 23$ so -2023 div 33 equals 23.
b) Since

$$\begin{aligned} (20234 - 2023) \bmod 25 &= (20234 \bmod 25 - 2023 \bmod 25) \bmod 25 \\ &= (9 - 23) \bmod 25 = 11 \end{aligned}$$

So the answer is 11.

c) Since

$$\begin{aligned} 94232 \cdot 2982 \bmod 7 &= \big((94323 \bmod 7) \cdot (2982) \bmod 7\big) \bmod 7 \\ &= (9 \cdot 0) \bmod 7 = 0 \end{aligned}$$

So the answer is 0.

PROBLEM 3. Transfer the following integer into another base.

SOLUTION. **a)** The binary number can be expressed in

$$(11011)_2 = 1 \cdot 2^4 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 27$$

b) The binary number can be expressed in three digits per group form

$$(101100)_2 = 101\ 100 = 5\ 4 = (54)_8$$

c) The digits of hexadecimal can be expressed in four digits of binary each

$$\begin{aligned} (AE01F)_{16} &= A\ E\ 0\ 1\ F \\ &= 1010\ 1110\ 0000\ 0001\ 1111 \\ &= (10101110000000011111)_2 \end{aligned}$$

d) The octal can be expressed in binary and then in hexadecimal

$$\begin{aligned} (720235)_8 &= 7\ 2\ 0\ 2\ 3\ 5 \\ &= 111\ 010\ 000\ 010\ 011\ 101 \\ &= 0011\ 1010\ 0000\ 1001\ 1101 \\ &= 3\ A\ 0\ 9\ D = (3A09D)_{16} \end{aligned}$$

PROBLEM 4. Find the prime factorization of the following integers.

SOLUTION. **a)** Iterate from 2 to $\sqrt{8085} = 90$ and test if the factors are prime, we got

$$8085 = 3 \times 5 \times 7^2 \times 11$$

b) Since 12! is factorial, we have

$$\begin{aligned} 12! &= 12 \times 11 \times \cdots \times 1 \\ &= 2^{10} \times 3^5 \times 5^2 \times 7 \times 11 \end{aligned}$$

PROBLEM 5. Apply the (Extended) Euclidean algorithm.

SOLUTION. **a)** The steps are shown below

$$\begin{aligned} &\text{Step1: } 267 = 3 \cdot 79 + 30 \\ &\text{Step2: } 79 = 2 \cdot 30 + 19 \\ &\text{Step3: } 30 = 19 + 11 \\ &\text{Step4: } 19 = 11 + 7 \\ &\text{Step5: } 11 = 7 + 4 \\ &\text{Step6: } 7 = 4 + 3 \\ &\text{Step7: } 4 = 3 + 1 \\ &\text{Step8: } 3 = 3 \cdot 1 \end{aligned}$$

the value of $\gcd(267, 79)$ is 1.

b) Find the coefficients using the extended gcd algorithm to solve

$$s \cdot 267 + t \cdot 79 = \gcd(267, 79)$$

and we got $s = 29$, $t = -98$, which is the solution.

c) From the previous solution we could know that

$$3 \cdot (29 \cdot 267 + -98 \cdot 79) = 3 \cdot 1$$

thus, we got the solution of this congruence, $x = 3 \cdot 29 = 87$

d) The extended gcd algorithm can be used to find the Bézout coefficients, that is

$$252x + 356y = \gcd(252, 356)$$

And the steps are

$$\begin{aligned}
&\text{Step1: } 252x + 356y = \gcd(252, 356) \\
&\text{Step2: } 252x_0 + 104y_0 = \gcd(252, 104) \\
&\text{Step3: } 104x_1 + 44y_1 = \gcd(104, 44) \\
&\text{Step4: } 44x_2 + 16y_2 = \gcd(44, 16) \\
&\text{Step5: } 16x_3 + 12y_3 = \gcd(16, 12) \\
&\text{Step6: } 12x_4 + 4y_4 = \gcd(12, 4) \\
&\text{Step8: } 4x_5 + 0y_5 = 0
\end{aligned}$$

where the solutions of each equations are

$$x_i = y_{i+1} \quad y_i = x_{i+1} - (a \text{ div } b) \cdot y_{i+1}$$

and we got the solution

$$x = -24 \quad y = 17 \quad \gcd(252, 356) = 4$$

Thus, the combination is

$$\gcd(252, 356) = -24 \cdot 252 + 17 \cdot 356$$

Problem 6. Prove that if $c \mid ab$ then $c \mid a \cdot \gcd(b, c)$.

Solution. According to the Bézout's Theorem, we have

$$bx + cy = \gcd(b, c)$$

And from the premise,

$$ab = ck,\ \ k \in \mathbb{Z}$$

So,

$$\begin{aligned} a \cdot \gcd(b, c) &= a \cdot (bx + cy) \\ &= abx + acy \\ &= kcx + acy \\ &= c \cdot (kx + ay) \end{aligned}$$

which can obvious be divided by c.

Problem 7. Prove the following statements using the fact that if a and m are coprime, then there exists an inverse of a modulo m.

Solution. **a)** Suppose that x and y are arbitary two inverses of a modulo m, then we have

$$ax \equiv 1 \mod m \quad \text{and} \quad ay \equiv 1 \mod m$$

and the difference of them is

$$\begin{aligned} ax \bmod m - ay \bmod m &= 0 \bmod m \\ ax - ay \bmod m &= 0 \bmod m \\ a(x - y) \bmod m &= 0 \bmod m \end{aligned}$$

since $\gcd(a, m) = 1$, we can derive that $x - y = 0$. Thus, $x = y$, which means the inverse is unique.

b) Suppose that there exists an inverse k, then

$$ak + my = 1$$

since

$$\gcd(a, m) \mid a, m$$

we got

$$\begin{aligned} &\gcd(a, m) \mid ak + my \\ \Rightarrow &\gcd(a, m) \mid 1 \end{aligned}$$

which is contradict to the premise. Thus, by contradiction, the inverse does not exist for $\gcd(a, m)$

PROBLEM 8. Prove the uniqueness of the solution of system of linear congruences.

SOLUTION. **a)** At first, we shall prove that if m, n are coprime then

$$\begin{cases} a \equiv b \mod n \\ a \equiv b \mod m \end{cases} \Rightarrow a \equiv b \mod mn$$

Proof: Since

$$\begin{cases} a \equiv b \mod n \\ a \equiv b \mod m \end{cases}$$

we have

$$\begin{cases} a - b &= k_1 m \\ a - b &= k_2 n \end{cases} \Rightarrow k_1 m = k_2 n$$

and therefore, $n \mid k_1 m$ and since m, n are coprime, $n \mid k_1$.
Let $k_1 = qn$, we have

$$a - b = q \cdot mn \Rightarrow a \equiv b \mod mn$$

Therefore, if

$$a \equiv b \mod m_i \quad i \in [1, n]$$

it's obvious that

$$a \equiv b \mod m_1 m_2 \cdots m_n$$

which is

$$a \equiv b \mod m$$

b) Suppose there exists another solution x', then

$$x \equiv x' \mod m_1$$
$$x \equiv x' \mod m_1$$
$$\dots$$
$$x \equiv x' \mod m_n$$

from (a) we can derive that

$$x \equiv x' \mod m$$

which means x' does not exist under the modulo m. So the solution is unique.

Problem 9. Solve the system of linear congruences.

Solution. **a)** At first, we can prove that if m has factors m_1, m_2 then

$$a \equiv b \pmod{m} \rightarrow a \equiv b \pmod{m_1} \text{ and } a \equiv b \pmod{m_2}$$

Proof

$$\begin{aligned}
&a - b = km \\
&\to a - b = km_1 m_2 \\
&\to a \equiv b \mod m_1 \\
&\to a \equiv b \mod m_2
\end{aligned}$$

So the system can be tranformed into

$$\begin{cases}
x \equiv 5 \pmod 2 \\
x \equiv 3 \pmod 5 \\
x \equiv 8 \pmod 7
\end{cases}$$

b) Find the solution using Chinese Remainder Theroem

$$\begin{aligned}
m &= 2 \cdot 5 \cdot 7 = 70 \\
M_1 &= 5 \cdot 7 = 35 \\
M_2 &= 2 \cdot 7 = 14 \\
M_3 &= 2 \cdot 5 = 10
\end{aligned}$$

the inverses are

$$\begin{aligned}
y_1 &= 1 \\
y_2 &= 4 \\
y_3 &= 5
\end{aligned}$$

so the solution is

$$x = 5 \cdot 35 \cdot 1 + 3 \cdot 14 \cdot 4 + 8 \cdot 10 \cdot 5 = 743$$

Problem 10. Prove the Fermat's little theorem.

Solution. **a)** Suppose there exists $i, j \in \{1, 2, \cdots, p-1\}$ and $i \neq j$, such that

$$ai \equiv aj \mod p$$

then we have

$$p \mid (ai - aj)$$

since a is not divisible by p and $i - j < p$ and p is prime, it's impossible. Thus, by contradiction, i and j do not exist and no two of the integers $1 \cdot a, 2 \cdot a, \cdots, (p-1) \cdot a$ are congruent modulo p.

b) Since p is prime and $\phi(p) = p - 1$, the set

$$A = \{i \bmod p \big| i \in [1, p-1]\}$$

has cardinality $|A| = p - 1$ and from (a) we know that the set

$$B = \{a \cdot i \bmod p \big| i \in [1, p-1]\}$$

has the same cardinality $p - 1$.

So, there exists a bijection between A and B, which is

$$ai \equiv j \mod p$$

where $i, j \in [1, p-1]$ and $i \neq j$. Thus, the product of them is

$$\begin{aligned} & 1 \cdot 2 \cdots p - 1 \equiv 1 \cdot a \cdot 2 \cdot a \cdots p - 1 \cdot a \mod p \\ \Rightarrow \quad & (p-1)! \equiv a^{p-1}(p-1)! \mod p \end{aligned}$$

c) Since $p \nmid (p-1)!$ the result of (b) can be transfered into

$$a^{p-1} \equiv 1 \mod p$$

by dividing both side with $(p-1)!$.

d) Since $p \nmid a$, we could multiply both side by a, that is

$$a^p \equiv a \mod p$$

Problem 11. Evaluate the following quantities with indicated method.

Solution. **a)** From the Fermat's little theorem,

$$5^6 \equiv 1 \mod 7$$

and we have

$$\begin{aligned} 5^{2023} \bmod 7 &= ((5^6 \bmod 7)^{337} \cdot 5) \bmod 7 \\ &= 5 \bmod 7 = 5 \end{aligned}$$

So the answer is 5.

b) According to Euler's theorem,

$$8^{\phi(15)} = 8^{10} \equiv 1 \mod 15$$

and we have

$$\begin{aligned} 8^{2023} \bmod 15 &= \big((8^10 \bmod 15)^{202} \cdot (8^3 \bmod 15)\big) \bmod 15 \\ &= 512 \bmod 15 = 2 \end{aligned}$$

So the answer is 2.

Problem 12. Consider a situation where we use RSA encryption with $(n, e) = (65, 7)$, explain the whole process.

SOLUTION. **a)** The encrypted message of M is

$$
\begin{aligned}
C &= M^e \mod n \\
\Rightarrow C &= 57
\end{aligned}
$$

b) Get the Euler's ϕ of n first, it's obvious that n is prime

$$\phi = n - 1 = 64$$

and solving the linear congruence equation

$$ed \equiv 1 \mod 64$$

could get

$$d = 55$$

c) The decryption of the ciphertext is

$$
\begin{aligned}
D &= C^d \mod n \\
\Rightarrow D &= 8 \\
&= M
\end{aligned}
$$