Discrete Structures :: CS 207 :: Autumn 2020

Problem Set 3b

Released: August 29, 2021

1. **Extended Euclidean Algorithm.** Consider the following recursive description of Euclid's GCD algorithm.

   [1] Euclid$a \in \mathbb{Z}^+, b \in \mathbb{Z}^+$ $a > b$ $\textsc{Euclid}(b, a)$ In the following, we assume $a \leq b$ $a|b$ a $(q, r) \leftarrow \textsc{Divide}(b, a)$ $\textsc{Divide}(c, d)$ returns (q, r) such that $c = dq + r$, where $0 \leq r < |d|$ $\textsc{Euclid}(r, a)$

   (a) Modify the above function to return a pair of integers (u, v) such that $au + bv = \gcd(a, b)$.

   Solution: The modified lines are shown in colour. [1] Euclid$a \in \mathbb{Z}^+, b \in \mathbb{Z}^+$ $a > b$ $\textsc{Euclid}(b, a)$ In the following, we assume $a \leq b$ $a|b$ $(1, 0)$ $\gcd(a, b) = a = a \cdot 1 + b \cdot 0$. $(q, r) \leftarrow \textsc{Divide}(b, a)$ $\textsc{Divide}(c, d)$ returns (q, r) such that $c = dq + r$, where $0 \leq r < |d|$ $(u, v) \leftarrow \textsc{Euclid}(r, a)$ $(v - qu, u)$ $\gcd(a, b) = \gcd(r, a) = ru + av = (b - aq)u + av = a(v - qu) + bu$

   (b) Compute the output of our modified function on the input pair $(1918, 2019)$.

   Hint: You can use a table with three columns for the input (a, b), the intermediate value (q, r) and the output (u, v), for each call to the function. You would fill the first two columns from top to bottom, and the last column in the reverse direction.

   Solution:

(a, b)	(q, r)	(u, v)
$(1918, 2019)$	$(1, 101)$	
$(101, 1918)$	$(18, 100)$	
$(100, 101)$	$(1, 1)$	
$(1, 100)$	base case	$(1, 0)$

   $\rightarrow$

(a, b)	(q, r)	(u, v)
$(1918, 2019)$	$(1, 101)$	$(-20, 19)$
$(101, 1918)$	$(18, 100)$	$(19, -1)$
$(100, 101)$	$(1, 1)$	$(-1, 1)$
$(1, 100)$	base case	$(1, 0)$

   The output is $(-20, 19)$.

2. Prove that $\phi(3n) = 2\phi(n)$ if and only if 3 does not divide n. (For this claim to hold for all $n \in \mathbb{Z}^+$, use the convention that $\phi(1) = 1$.)

   Solution: First, we show that if 3 does not divide n then $\phi(3n) = 2\phi(n)$. Since 3 and n are coprime, we can write

   $$\phi(3n) = \phi(3)\phi(n) = (3 - 1)\phi(n) = 2\phi(n)$$

   (This holds for all $n \in \mathbb{Z}^+$, where, by convention, $\phi(1) = 1$.)

   Now we prove the other side, i.e., if $\phi(3n) = 2\phi(n)$ then 3 does not divide n. Let's assume for the sake of contradiction that 3 divides n i.e. $n = 3^k l$ where $k, l \geq 1$ and 3 does not divide l. It follows that

   $$\phi(3n) = \phi(3^{k+1} l) = \phi(3^{k+1})\phi(l) = 2.3^k \phi(l)$$

   On the other hand,

   $$2\phi(n) = 2\phi(3^k l) = 2\phi(3^k)\phi(l) = 2^2 3^{k-1}\phi(l) \neq 2 \cdot 3^k \phi(l) = \phi(3n)$$

   We have reached a contradiction.

3. Find all $n \in \mathbb{Z}^+$ such that $\phi(n)$ is not divisible by 4.

   Solution: According to the fundamental theorem of arithematic, any integer $n \geq 2$ can be written as $n = p_1^{k_1} p_2^{k_2} \ldots p_l^{k_l}$ where $p_1, p_2, \ldots p_l$ are distinct primes, $k_1, k_2, \ldots k_l \geq 1$ and $l \geq 1$. It follows that

   $$\begin{aligned}\phi(n) &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_l}\right) \\ &= \frac{n(p_1 - 1)(p_2 - 1)\ldots(p_l - 1)}{p_1 p_2 \ldots p_l} \\ &= p_1^{k_1 - 1} p_2^{k_2 - 1} \ldots p_l^{k_l - 1}(p_1 - 1)(p_2 - 1)...(p_l - 1)\end{aligned}$$

   Let's assume that n has at least 2 odd prime factors, say p_i and p_j. Then $\phi(n)$ will have at least 2 even terms in the expansion above, $p_i - 1$ and $p_j - 1$ and hence will be divisible by 4. Thus, there can be at most 1 odd prime factor of n, let's say p.

   Also, $p \equiv 3 \pmod 4$. This is because if $p \equiv 1 \pmod 4$, then $p - 1$ will be divisible by 4. Also, there is no other possibility modulo 4 for p as it is odd.

Thus, $n = 2^{k_1} p^{k_2}$ where $p \equiv 3 \pmod 4$. Then,

$$\phi(n) = 2^{k_1-1} p^{k_2-1}(p-1)$$

if $k_1, k_2 \geq 1$ and

$$\phi(n) = 2^{k_1-1}$$

if $k_1 \geq 1$ and $k_2 = 0$. In the first case, $k_1 - 1 \leq 0$ because 2 divides $p-1$. In the second case, $k_1 - 1 \leq 1$.

Hence, the possibilities for such n are 1, 2, 4, p^k or $2p^k$ where $p \equiv 3 \pmod 4$ and $k \geq 1$.

4. Find all $n \in \mathbb{Z}^+$ such that $\phi(n)|n$.

Solution: Any integer $n \geq 2$ has a unique representation as a product of prime numbers i.e. $n = p_1^{k_1} p_2^{k_2} \ldots p_\ell^{k_\ell}$ where $p_1, p_2, \ldots p_\ell$ are distinct primes, $k_1, k_2, \ldots k_\ell \geq 1$ and $\ell \geq 1$. It follows that

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_\ell}\right) = \frac{n(p_1-1)(p_2-1)\ldots(p_\ell-1)}{p_1 p_2 \ldots p_\ell}$$

In other words, we can write $n = \frac{N}{D}\phi(n)$, where

$$N = p_1 p_2 \ldots p_\ell$$

and

$$D = (p_1-1)(p_2-1)\ldots(p_\ell-1)$$

It follows that $\phi(n)|n$ iff $D|N$.

Suppose that n is divisible by at least 2 distinct odd primes, say p_i and p_j. Then, $D \equiv 0 \pmod 4$ (for an odd prime p, $p-1$ is even), but $N \equiv 2 \pmod 4$ or N is odd, contradicting the requirement that $D|N$. Therefore, it can be assumed that n is divisible by at most one odd prime, say p. So, $n = 2^{k_1} p^{k_2}$ for an odd prime p and $k_1, k_2 \geq 0$. We consider the following cases:

Case $k_2 = 0$: In this case $n = 2^{k_1}$. If $k_1 > 0$, $\phi(n) = n/2$ and if $k_1 = 0$, then $n = 1$ and $\phi(n) = 1$. In both cases $\phi(n)|n$.

Case $k_2 > 0$: Now, if $k_1 = 0$, we have $n = p^{k_2}$ then $N = p$ and $D = p - 1$. For N to be divisible by D, it must be the case that $p = 2$ but this contradicts the fact that p is an odd prime.
If $k_1 > 0$ then $N = 2p$ and $D = p - 1$. For N to be divisible by D, the only possibility is if $p = 3$ as p and $p - 1$ are always co-prime.

Thus $\phi(n)|n$ iff n is of the form 2^k for $k \geq 0$ or $2^{k_1} 3^{k_2}$ where $k_1, k_2 > 0$.

5. Define the *order* of $a \in \mathbb{Z}_m^*$ to be

$$\text{ord}(a, m) = \min\{d > 0 | a^d \equiv 1 \pmod m\}.$$

Prove that for every $a \in \mathbb{Z}_m^*$, $\text{ord}(a, m)|\phi(m)$.

Hint: Use Euler's Totient theorem. If $\text{ord}(a, m)$ *does not divide* $\phi(m)$*, what can you say about its remainder?*

Solution: For $a \in \mathbb{Z}_m^*$, let $S = \{d > 0 | a^d \equiv 1 \pmod m\}$ and g be $\text{ord}(a, m)$, that is, the minimum element in S.

We prove that g divides $\phi(m)$ by contradiction.

Suppose, for the sake of contradiction, g doesn't divide $\phi(m)$. That is,

$$\phi(m) = gq_1 + r_1$$

where q_1 is the quotient and $0 < r_1 < g$.

Consider,

$$\begin{aligned} a^{\phi(m)} &\equiv a^{gq_1 + r_1} \pmod m \\ &\equiv (a^g)^{q_1} \cdot a^{r_1} \pmod m \\ &\equiv (1)^{q_1} \cdot a^{r_1} \pmod m && \text{since } g \in S \\ &\equiv a^{r_1} \pmod m \end{aligned}$$

But by Euler's Totient theorem, we have, $a^{\phi(m)} \text{mod m} = 1$.

This implies, $a^{r_1} \text{mod m} = 1$ and $r_1 > 0$. Therefore, r_1 must be in S. But as $r_1 < g$, this contradicts the minimality of g. Therefore, our assumption is false and hence order(a, m) divides $\phi(m)$.

6. Define the *maximum order* in $\mathbb{Z}_m^*$ to be
$$\text{maxord}(m) = \max_{a \in \mathbb{Z}_m^*} \text{ord}(a, m).$$
In the lectures, it was mentioned that for many m, $\text{maxord}(m) = \phi(m)$. In particular, this is the case when m is of the form p^k for odd primes p. In this problem you explore some cases when it is not so.

   (a) What is maxord(8)? Compute this by enumerating $\text{ord}(a, 8)$ for all $a \in \mathbb{Z}_8^*$.
   Solution: We have $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$. The corresponding order of these elements modulo 8 are $\{1, 2, 2, 2\}$. Hence $\text{maxord}(8) = 2$.

   (b) Suppose p, q are distinct primes. Let $r = \text{maxord}(p)$ and $s = \text{maxord}(q)$. Prove that $\text{maxord}(pq) = \text{lcm}(r, s)$.
   Hint: Use CRT. To prove that $\text{maxord}(pq) = d$ *you can show that* $\forall a \in \mathbb{Z}_{pq}^*$, $a^d = 1$ and $\exists a \in \mathbb{Z}_{pq}^*$ *s.t.* $\text{ord}(a) = d$.
   Solution: Firstly, recall the fact that when p is a prime, $\mathbb{Z}_p^*$ has a generator, say g. Then $\text{ord}(g, p) = p - 1$. On the other hand, for all $a \in \mathbb{Z}_p^*$, by Fermat's little theorem, $a^{p-1} \equiv 1 \pmod p$, and hence $\text{ord}(a, p) \le p - 1$. Thus $\text{maxord}(p) = p - 1$. Similarly, $\text{maxord}(q) = q - 1$.
   Let $d = \text{lcm}(r, s)$, where $r = p - 1$, $s = q - 1$. We shall show that $\text{maxord}(pq) = d$.
   To show that $\text{maxord}(pq) \le d$, consider an arbitrary $a \in \mathbb{Z}_{pq}^*$. Since $r|d$ and $s|d$, by Fermat's little theorem we have $a^d \equiv 1 \pmod p$ and $a^d \equiv 1 \pmod q$. Thus the CRT representation of $a^d \in \mathbb{Z}_{pq}^*$ is $(1, 1) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$. Since $(1, 1)$ is the CRT representation of 1, $a^d \equiv 1 \pmod{pq}$. Thus $\text{ord}(a, pq) \le d$. Since this holds for all $a \in \mathbb{Z}_{pq}^*$, $\text{maxord}(pq) \le d$.
   To show that $\text{maxord}(pq) \ge d$, we shall find one element z such that $\text{ord}(z, pq) \ge d$. Let g and h be generators of $\mathbb{Z}_p^*$ and $\mathbb{Z}_q^*$, respectively. We define z to be the element with CRT representation (g, h). Now, suppose $\text{ord}(z, pq) = t$. Then, $t > 0$ and $z^t \equiv 1 \pmod{pq}$. Then, by CRT $g^t \equiv 1 \pmod p$ and $h^t \equiv 1 \pmod q$. Since g, h are generators, this requires $r|t$ and $s|t$. But $d = \text{lcm}(r, s)$ is the smallest positive common multiple of r, s. Hence $t \ge d$. Thus, $\text{ord}(z, pq) \ge d$ as required.

   (c) Use part (b) to argue that when p, q are two distinct odd primes, $\text{maxord}(p, q) \ne \phi(pq)$.
   Solution: From (b) we have, $\text{maxord}(p, q) = \text{lcm}(\text{maxord}(p), \text{maxord}(q)) = \text{lcm}(p - 1, q - 1)$. On the other hand, $\phi(pq) = (p - 1)(q - 1)$. Since p, q are odd, 2 is a common factor of $p - 1$ and $q - 1$ and hence $\text{lcm}(p - 1, q - 1) = pq/\gcd(p - 1, q - 1) \le (p - 1)(q - 1)/2$. Hence $\text{maxord}(pq) \ne \phi(pq)$.

7. If possible, solve the following system of congruences using the Chinese Remainder theorem :
$$2x \equiv 11 \pmod{23}$$
$$9x \equiv 12 \pmod{31}$$
Hint: First write this system in a form to which CRT applies.

Solution:

We first rewrite the equations in a form where CRT can be applied.

We note that inverse of 2 modulo 23 is 12 and inverse of 9 modulo 31 is 7.

Therfore, multiplying the first equation by 12 and the second by 7, we get,
$$x \equiv 11 \cdot 12 \pmod{23}$$
$$x \equiv 12 \cdot 7 \pmod{31}$$
Which are equivalent by modulo arithmetic to,
$$x \equiv 17 \pmod{23}$$
$$x \equiv 22 \pmod{31}$$
Now, as $\gcd(23, 31) = 1$, we have a unique solution modulo $(23 \cdot 31)$ to the above system. We shall find integers u, v such that $23u + 31v = 1$, and then we can set $x = 31 \cdot v \cdot 17 + 23 \cdot u \cdot 22$. For this, we execute the Extended Euclidean Algorithm, and go through the following sequence of pairs:
$$(23, 31) \to (23, 8 = 31 - 23) \to (7 = 23 - 2 \cdot 8, 8) \to (7, 1 = 8 - 7).$$
Working backwards, we have $1 = 8 - 7 = 8 - (23 - 2 \cdot 8) = 3 \cdot 8 - 23 = 3(31 - 23) - 23 = 3 \cdot 31 - 4 \cdot 23$. That is, $u = -4$ and $v = 3$. Hence, we set
$$x = 31 \cdot 3 \cdot 17 + 23 \cdot (-4) \cdot 22 = -443$$
, or $x \equiv 270 \pmod{713}$.

8. Solve the following system of congruences :

$$\begin{aligned} 2x + 5y &\equiv 4 \pmod{11} \\ x + 3y &\equiv 7 \pmod{11} \end{aligned}$$

Hint: How would you solve such a system over the real or rational numbers, instead of modulo 11? You can proceed similarly, 11 being a prime.

Solution:

Subtracting the first equation from 2 times the second equation, we have

$$y \equiv 2 \cdot 7 - 4 \pmod{11}.$$

That is $y \equiv 10 \pmod{11}$. Substituting this into the second equation, we have $x \equiv 7 - 30 \pmod{11}$. That is, $x \equiv 10 \pmod{11}$.

9. Find the last 2 digits of 2^{2018}.

Hint: Note that 2 is not coprime with 100.

Solution: We need to find $2^{2018} \pmod{100}$. But since 2 is not coprime to 100, we cannot apply Euler's Theorem directly. Instead, we find 2^{2018} modulo 25 and modulo 4 separately, and then use CRT to combine them.

By Euler's Theorem,

$$2^{20} \equiv 1 \pmod{25}$$

because $\phi(25) = 20$. Since $2018 \equiv -2 \pmod{20}$, we have

$$\begin{aligned} 2^{2018} &\equiv 2^{20q-2} \pmod{25} && \text{for some } q \\ &\equiv 13^2 \pmod{25} && \text{since } 2^{-1} \equiv 13 \pmod{25} \\ &\equiv 19 \pmod{25} && \text{since } 13^2 = 169 = 150 + 19. \end{aligned}$$

Also, $2^{2018} \equiv 0 \pmod{4}$. While one can solve for x s.t., $x \equiv 19 \pmod{25}$ and $x \equiv 0 \pmod{4}$, in this case it is easier to enumerate the four values of $x \pmod{100}$ which satisfies the first congruence: $19, 44, 69, 94$ and note that 44 is the one which satisfies the second congruence. Thus the last two digits of 2^{2018} are 44.

10. **Square-Roots of 1.** In the lecture, we discussed the square-roots of 1 modulo a prime number.

(a) Find all solutions of $x^2 \equiv 1 \pmod{p^k}$ where p is prime and $k \geq 1$.

Hint: Separately analyze the cases when p is odd and $p = 2$.

Solution: Firstly, $x^2 \equiv 1 \pmod{m}$ iff $(x+1)(x-1) \equiv 0 \pmod{m}$. That is $m|(x+1)(x-1)$. When $m = p^k$ where p is a prime, this means that $p^i|(x+1)$ and $p^j|(x-1)$ for some i, j such that $i + j \geq k$.

Following the hint, we treat the cases when p is even and odd separately.

Case 1: p is odd. We cannot have $p|(x+1)$ and $p|(x-1)$, because otherwise $p|2$. Hence, either $p^k|(x+1)$ or $p^k|(x-1)$. Correspondingly, we require $x \equiv \pm 1 \pmod{p^k}$. In either case, $x^2 \equiv 1 \pmod{p^k}$. So these are exactly the two possible solutions.

Case 2: $p = 2$. Suppose $2^i|(x+1)$ and $2^j|(x-1)$. Note that if $i \geq 2$ and $j \geq 2$, then $4|(x+1)$ and $4|(x-1)$, which implies that $4|2$, a contradiction. So we have the following 4 cases where at least one of i, j is < 2:

- $i = 0$. In this case $j \geq k$, and so $2^k|(x-1)$. That is $x \equiv 1 \pmod{2^k}$.
- $i = 1$. In this case $j \geq k - 1$, and so $2^{k-1}|(x-1)$. That is $x - 1 = q2^{k-1}$. If q is even, have $x \equiv 1 \pmod{2^k}$ as in the previous case. Otherwise, $x \equiv 2^{k-1} + 1 \pmod{2^k}$.
- $i \geq k - 1, j = 1$. In this case, working as above, we get $x \equiv -1 \pmod{2^k}$ or $x \equiv 2^{k-1} - 1 \pmod{2^k}$.
- $i \geq k, j = 0$. In this case, working as above, we get $x \equiv -1 \pmod{2^k}$.

Thus, for $m = 2^k$, the set of possible solutions for the congruence $x^2 \equiv 1 \pmod{m}$ are $\{\pm 1, \frac{m}{2} \pm 1\}$. We note that all these values indeed satisfy the congruence.

(b) Find all solutions of $x^2 \equiv 1 \pmod{144}$.

Solution: By CRT, $x^2 \equiv 1 \pmod{144}$ if and only if x satisfies the system of congruences $x^2 \equiv 1 \pmod{16}$ and $x^2 \equiv 1 \pmod{9}$. From (a), solutions to the $x^2 \equiv 1 \pmod{16}$ are $1, -1, 7, 9 \pmod{16}$ and solutions to the $x^2 \equiv 1 \pmod{9}$ are $1, -1 \pmod{9}$. That is, the set of solutions of $x^2 \equiv 1 \pmod{144}$ are exactly those which satisfy

$$x \equiv 1, -1, 7 \text{ or } 9 \pmod{16}$$
$$x \equiv 1, -1 \pmod{9}.$$

Each of the 8 pairs in $\{\pm 1, 8 \pm 1\} \times \{\pm 1\}$ corresponds to the CRT representation of a unique x modulo 144. Using the fact that $16 \cdot 4 + 9 \cdot (-7) = 1$, we obtain these 8 solutions as 1, 127, 55, 73, 17, 143, 71, 89.