Solutions to practice problems for Midterm 1

1. Find the gcd of 621 and 483.

   Solution: We run the Euclidean algorithm:

$$
\begin{aligned}
621 &= \mathbf{1} \cdot 483 + 138 \\
483 &= \mathbf{3} \cdot 138 + 69 \\
138 &= 2 \cdot 69.
\end{aligned}
$$

   So $\gcd(621, 483) = 69$.

2. Find a solution of $621m + 483n = k$, where k is the gcd of 621 and 483.

   Solution: Building upon problem 1, we extend the table:

$$
\begin{array}{r|rr|r}
1 & 1 & 0 & 621 \\
1 & 0 & 1 & 483 \\
3 & 1 & -1 & 138 \\
\hline
 & -3 & 4 & 69
\end{array}
$$

   So $-3 \cdot 621 + 4 \cdot 638 = 69$, i.e. $(m, n) = (-3, 4)$ works.

3. Calculate 3^{64} modulo 67 by repeated squaring.

   Solution: We have

$$
\begin{aligned}
3^4 = 81 &\equiv 14 \pmod{67} \\
3^8 \equiv 14^2 = 196 &\equiv -5 \pmod{67} \\
3^{16} \equiv 5^2 &\equiv 25 \pmod{67} \\
3^{32} \equiv 25^2 = 625 &\equiv 22 \pmod{67} \\
3^{64} \equiv 22^2 = 484 &\equiv 15 \quad \text{mod } 67.
\end{aligned}
$$

4. Calculate 3^{64} modulo 67 using Fermat's little theorem.

   Solution: We know $3^{66} \equiv 1 \pmod{67}$. So

$$3^2 \cdot 3^{64} \equiv 1 \pmod{67}$$

   . so we just need to invert 9 mod 67. You can either do this by the Euclidean algorithm, or by inspection. For example, $67 \cdot 2 + 1 = 135 = 15.9$, so it follows that $9^{-1} \equiv 15 \pmod{67}$.

5. Calculate $\phi(576)$.

   Solution: The factorization is $576 = 24^2 = 2^6 \cdot 3^2$. So $\phi(576) = 2^5 \cdot 3 \cdot 2 = 192$.

6. Find all the solutions of $x^3 - x + 1 \equiv 0 \pmod{25}$. Let $f(x) = x^3 - x + 1$. First we find solutions to $f(x) \equiv 0 \pmod 5$, just by trying all the values of x modulo 5. We see that $x \equiv -2 \pmod 5$ is the only solution. Now we want to apply Hensel's lemma. We have

$f'(x) = 3x^2 - 1$ and $f'(-2) = 11 \equiv 1 \pmod 5$. So $\overline{f'(-2)} = f'(-2)^{-1} \equiv 1 \pmod 5$. Finally, $f(-2) = -5$, so the solution modulo 25 is

$$-2 - (-5) \cdot 1 = 3 \pmod 25.$$

We check that $3^3 - 3 + 1 = 25 \equiv 0 \pmod{25}$.

7. Find all solutions of $x^3 - x + 1 \equiv 0 \pmod{35}$.

   Solution: The idea is to solve it modulo 5 and 7 and then use the Chinese remainder theorem. The unique solutions modulo 5 and 7 are -2 and 2 , respectively. Also, we have $3 \cdot 5 - 2 \cdot 7 = 1$. So to combine the solutions, we take

$$15 \cdot 2 + (-14) \cdot (-2) = 30 + 28 = 58 \equiv 23 \pmod{35}.$$

8. Find the smallest integer N such that $\phi(n) \geq 5$ for all $n \geq N$.

   Solution: Trying out small values of n, we see that $\phi(12) = 4$ but $\phi(n)$ seems to be greater than 4 for all $n \geq 13$. Let's prove this: suppose $n \geq 11$. Let $n = \prod p_i^{e_i}$, so $\phi(n) = \prod p_i^{e_i - 1}(p_i - 1)$. Let e be the power of 2 dividing n. If $e \geq 4$, then $\phi(n) \geq 2^{e-1} \geq 8$. So we only need to consider $e = 0, 1, 2, 3$.

   If $e = 0$, then n is odd. If n is prime, then $\phi(n) = n - 1 \geq 12$. Otherwise, either n will be divisible by at least two distinct odd primes p and q, in which case $\phi(n) \geq (p-1)(q-1) \geq 2 \cdot 4 = 8$, or n is divisible by p^2 for some odd prime p, in which case $\phi(n) \geq p(p-1) \geq 3(3-1) = 6$.

   Next suppose $e = 1$. Then $n = 2m$ where m is odd and $m = n/2 \geq 7$. We have $\phi(n) = \phi(m)$. Then if m is prime, $\phi(n) = m - 1 \geq 6$. Otherwise, the above reasoning (for the $e = 0$ case) shows that $\phi(n) \geq 6$.

   Next, the case $e = 2$. Then $n = 4m$, with m odd and $m = n/4 > 3$, so $m \geq 5$ since m is an odd integer. So $\phi(n) = 2\phi(m)$. As before we show that $\phi(m) \geq 4$, so $\phi(n) \geq 8$.

   Finally, if $e = 3$ then $n = 8m$, with m odd and $m = n/8 > 1$. So $m \geq 3$. Then $\phi(n) = 4\phi(m) = 4 \cdot 2 = 8$.

9. Find two positive integers m, n such that $\phi(mn) \neq \phi(m)\phi(n)$.

   Solution: In fact, any two integers which are not coprime will do! For example, $m = n = 2$ gives $\phi(m) = \phi(n) = 1$ and $\phi(mn) = 2$.

10. True or false: two positive integers m, n are coprime if and only if $\phi(mn) = \phi(m)\phi(n)$. Give a proof or counterexample.

    Solution: This is true. Let p_i (for $i \in I$) be the common primes dividing both m and n. Let q_j (for $j \in J$) be the primes dividing m but not n, and let r_k (for $k \in K$) be the primes dividing n but not m.

$$m = \prod p_i^{e_i} \prod q_j^{f_j}$$

and

$$n = \prod p_i^{f_i} \prod r_k^{h_k}.$$

Then calculating $\phi(m)$, $\phi(n)$ and $\phi(mn)$ gives

$$\frac{\phi(m)\phi(n)}{\phi(mn)} = \prod \left(1 - \frac{1}{p_i}\right).$$

Since $1 - 1/p_i < 1$, the only way this product could be 1 is if its is empty, i.e. if there are no common primes dividing m and n.

11. Give the definition of a reduced residue system modulo n.

12. State and prove the Chinese remainder theorem.

13. Show that $(n-1)! \equiv 0 \pmod{n}$ for composite $n > 4$. [Hint: Make sure that your proof works for the case $n = p^2$, where p is a prime].

    Solution: Let p be the smallest prime dividing n. If $n \neq p^2$ then p and n/p are both less than n and are distinct. So $(n-1)!$ is divisible by $p(n/p) = n$. Now, if $n = p^2$ then since $p > 2$ (because $n > 4$) we see that p and $2p$ are both less than n. So $(n-1)!$ is divisible by $p \cdot 2p = 2p^2 = 2n$ and therefore by n.

14. Solve the system of congruences

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{7} \end{aligned}$$

    Solution: We need to apply CRT. We have $3 \cdot 5 = 15 \equiv 1 \pmod{7}$, with inverse 1. Next, $3 \cdot 7 = 21 \equiv 1 \pmod{5}$, with inverse 1. Finally, $5 \cdot 7 = 35 \equiv -1 \pmod{3}$, with inverse -1. So the solution is

$$x \equiv 1 \cdot 35 \cdot (-1) + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 = -35 + 42 + 45 = 52 \pmod{105}.$$

15. Let n be a positive integer. Show the identity

$$\sum_{i=1}^{n} i \binom{n}{i} = n2^{n-1}.$$

    [Hint: differentiate both sides of the Binomial theorem, or manipulate the binomial coefficients.]

    Solution: We have $(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$. Differentiating we get

$$n(1+x)^{n-1} = \sum_{i=1}^{n} i \binom{n}{i} x^{i-1}$$

    where the $i = 0$ term goes away because differentiating a constant gives 0. Now plugging in $x = 1$, we get the result.

16. Calculate the order of 3 modulo 301.

    Solution: Note that $301 = 7 \cdot 43$. If h_1 is the order of 3 mod 7 and h_2 is the order of 3 mod 43, then the order of 3 mod 301 will just be the LCM (least common multiple of h_1 and h_2). Now, we know by Fermat that $3^6 \equiv 1 \pmod 7$. It's easy to see that 3^2 and 3^3 are not 1 modulo 7. So $h_1 = 6$. Also $3^{42} \equiv 1 \pmod{43}$. Since the order divides 42, it either equals 42 or divides $42/p$, where p is one of the primes dividing 42, namely $2, 3$ or 7. Now it's easy to check that $3^{21}, 3^{14}, 3^6$ are all not 1 mod 43. So $h_2 = 42$. Therefore $h_2 = 42$. Therefore the order of 3 mod 301 is $\mathrm{LCM}(6, 42) = 42$.

MIT OpenCourseWare
http://ocw.mit.edu

18.781 Theory of Numbers
Spring 2012

For information about citing these materials or our Terms of Use, visit: http://ocw.mit.edu/terms.