

Sample problems - Chapter 4 - Math 1350 - Fall 2010

There will be NO CALCULATORS for the final exam. There will be the usual list of letters and their corresponding numerical value. Also there will be the following instruction:

Trial and error methods which would not be effective for large numbers when other methods are available will receive at most half credit, even if 100% correct, and NO partial credit if incorrect.

1. Compute the greatest common divisor of 91 and 221.

We use the Euclidean algorithm.

$$\begin{aligned} 221 &= 2 \cdot 91 + 39 \\ 91 &= 2 \cdot 39 + 13 \\ 39 &= 3 \cdot 13 + 0. \end{aligned}$$

So the gcd is 13.

2. Compute $17^{-1} \pmod{48}$

Solution: We use the extended Euclidean algorithm.

$$\begin{aligned} 48 &= 2 \cdot 17 + 14 \\ 17 &= 1 \cdot 14 + 3 \\ 14 &= 4 \cdot 3 + 2 \\ 3 &= 2 + 1. \end{aligned}$$

Working backwards

$$\begin{aligned} 1 &= 1 \cdot 3 && - 1 \cdot 2 \\ &= 1 \cdot 3 && - 1 \cdot (14 - 4 \cdot 3) \\ &= 5 \cdot 3 && - 1 \cdot 14 \\ &= 5 \cdot (1 \cdot 17 - 1 \cdot 14) && - 1 \cdot 14 \\ &= 5 \cdot 17 && - 6 \cdot 14 \\ &= 5 \cdot 17 && - 6 \cdot (1 \cdot 48 - 2 \cdot 17) \\ &= 17 \cdot 17 && - 6 \cdot 48. \end{aligned}$$

So the answer is 17. Indeed, $17 \cdot 17 = 289 = 1 \pmod{48}$.

3. Compute $4^{21} \pmod{61}$.

Solution: First we write $21 = 16 + 4 + 1$ and then we start computing squares.

$$4^2 \pmod{61} = 16.$$

$$4^4 = 16^2 \pmod{61} = 256 \pmod{61} = 12.$$

$$4^8 = 12^2 \pmod{61} = 22.$$

$$4^{16} = 22^2 \text{ MOD } 61 = 57.$$

Hence, the answer will be $4 \cdot 12 \cdot 57 \text{ MOD } 61 = 48 \cdot 57 \text{ MOD } 61$
 $= 48 \cdot (-4) \text{ MOD } 61 = -192 \text{ MOD } 61 = -9 \text{ MOD } 61 = 52.$

Remark - this is definitely the most arithmetic you should expect to see on any problem and there might not be any that have this much. In general, errors in arithmetic (as opposed to method) will be punished very lightly.

4. Compute $7^{2012} \text{ MOD } 2011$. You may assume that 2011 is prime.

Solution: By the little Fermat theorem $7^{2010} \text{ MOD } 2011 = 1$. So, $7^{2012} = 7^{2010} \cdot 7^2 \text{ MOD } 2011 = 7^2 \text{ MOD } 2011 = 49$.

5. Compute $6^{50} \text{ MOD } 65$.

Solution: First we notice that $6 = 5 \cdot 13$ is a product of two primes and that 6 is relatively prime to 65. So, by Theorem 4.3.2 $6^{4 \cdot 12} \text{ MOD } 65 = 1$. Hence $6^{50} = 6^{48} \cdot 6^2 \text{ MOD } 65 = 6^2 \text{ MOD } 65 = 36$. Note: If you did not say that 6 was relatively prime to 65 you would definitely lose points.

6. Find the prime factorization of 9991.

Solution: 9991 is very close $10000 = 100^2$ and the difference $10000 - 9991 = 9 = 3^2$. So, by Fermat's factoring method $9991 = (100 - 3)(100 + 3) = 97 \cdot 103$. Since the last two are prime we are done.

7. Is 2 a primitive root mod 11? Is 3 a primitive root mod 11?

Solution: $2^2 = 4, 2^3 = 8, 2^4 = 5 \text{ MOD } 11, 2^5 = 10 \text{ MOD } 11, 2^6 = 9 \text{ MOD } 11, 2^7 = 7 \text{ MOD } 11, 2^8 = 3 \text{ MOD } 11, 2^9 = 6 \text{ MOD } 11$. Since they are all different 2 is a primitive root mod 11. Checking 3: $3^1 = 3, 3^2 = 9, 3^3 = 5 \text{ MOD } 11, 3^4 = 4 \text{ MOD } 11, 3^5 = 1 \text{ MOD } 11$ and $3^6 = 3 \text{ MOD } 11$. We already have a repeat, so 3 is not a primitive root mod 11.

8. A Diffie-Hellman key agreement protocol has been set up with public prime 29 and public base 2. Alice and Bob want to use this to generate a key for private communications. Alice sends Bob $\alpha = 16$. Bob chooses constant $b = 15$, so he sends Alice $2^{15} \text{ MOD } 29 = 27$. What is the agreed upon key?

Since $2^4 = 16 \text{ MOD } 29$ Alice's constant $a = 4$. Therefore, Bob can tell that the agreed key is $29^4 = (2^{15})^4 = 2^{60} \text{ MOD } 29$. By Fermat's little theorem $2^{28} = 1 \text{ MOD } 29$, so $2^{60} = 2^{28 \cdot 2 + 4} \text{ MOD } 29 = 2^4 \text{ MOD } 29 = 16$.

9. Find a solution to $120 \cdot n = 15 \text{ MOD } 195$. Hint: The gcd of 120 and 195 is 15.

Solution: This is just like finding multiplicative inverses, but with a gcd different than 1. Let's see what happens with the extended Euclidean algorithm.

$$\begin{aligned} 195 &= 1 \cdot 120 + 1 \cdot 75 \\ 120 &= 1 \cdot 75 + 1 \cdot 45 \\ 75 &= 1 \cdot 45 + 30 \\ 45 &= 1 \cdot 30 + 15. \end{aligned}$$

Reversing our steps

$$\begin{aligned} 15 &= 1 \cdot 45 && - 1 \cdot 30 \\ &= 1 \cdot 45 && - (1 \cdot 75 - 1 \cdot 45) \\ &= 2 \cdot 45 && - 1 \cdot 75 \\ &= 2 \cdot (1 \cdot 120 - 1 \cdot 75) && - 1 \cdot 75 \\ &= 2 \cdot 120 && - 3 \cdot 75 \\ &= 2 \cdot 120 && - 3 \cdot (1 \cdot 195 - 1 \cdot 120) \\ &= 5 \cdot 120 && - 3 \cdot 195. \end{aligned}$$

From the last line we can see that $120 \cdot 5 = 15 + 3 \cdot 195$, so $n = 5$ works.

Remark: This would be a typical of the hardest problem we might ask - something you could figure out how to do, but have never actually done.

10. Bob decides to use RSA encryption. He chooses $p = 13$ and $q = 23$, so he publishes 299 as his modulus ($299 = 13 \cdot 23$) and exponent $e = 121$. Is this a valid RSA scheme?

Solution: The encryption exponent must be relatively prime to $(p - 1) \cdot (q - 1) = 12 \cdot 22$. However, $121 = 11 \cdot 11$, so it is not relatively prime to 22. Therefore, this is not a valid RSA scheme.

11. Alice decides to use a Merkle-Hellman public key scheme. She uses the prime 97 with secret key $w = 49$. She publishes the sequence 50, 51, 5, 60, 21. If Bob wants to encipher the plaintext 10111 what is the cipher text? What was Alice's original superincreasing sequence?

Solution: We compute $w^{-1} \text{ MOD } 97$ with the extended Euclidean algorithm. This turns out to be 2 (We do not write it out here, but on the exam you would have to.) So the original superincreasing sequence is

$$\begin{aligned} 2 \cdot 50 \text{ MOD } 97 &= 3 \\ 2 \cdot 51 \text{ MOD } 97 &= 5 \\ 2 \cdot 5 \text{ MOD } 97 &= 10 \\ 2 \cdot 60 \text{ MOD } 97 &= 23 \\ 2 \cdot 21 \text{ MOD } 97 &= 42. \end{aligned}$$

To encipher 10111 Bob would send $50 + 5 + 60 + 21 = 136$.