Exam 2– 11/18/11
SOLUTIONS

Math 406

Name:

1. (15 points) If a general had 1200 troops at the start of the battle and if there were 3 left over when they lined up 5 at a time, 3 left over when they lined up 6 at a time, 1 left over when they lined up 7 at a time, and none left over when they lined up 11 at a time, how many troops remained after the battle?

We need to solve the simultaneous equations using the Chinese Remainder Theorem:

$$\begin{aligned} x &\equiv 3 \ (5) \\ x &\equiv 3 \ (6) \\ x &\equiv 1 \ (7) \\ x &\equiv 0 \ (11). \end{aligned}$$

For $m_1 = 5$, $M_1 = 6 \cdot 7 \cdot 11 \equiv 2 \ (5)$, which has inverse $y_1 = 3$ modulo 5.
For $m_2 = 6$, $M_2 = 5 \cdot 7 \cdot 11 \equiv 1 \ (6)$, so $y_2 = 1$.
For $m_3 = 7$, $M_3 = 5 \cdot 6 \cdot 11 \equiv 1 \ (7)$, so $y_3 = 1$.
We don't have to worry about the equation modulo 11, since $a_4 = 0$. Now we find a solution

$$\begin{aligned} x &= a_1 \cdot y_1 \cdot M_1 + a_2 \cdot y_2 \cdot M_2 + a_3 \cdot y_3 \cdot M_3 \\ &= 3 \cdot 3 \cdot (6 \cdot 7 \cdot 11) + 3 \cdot 1 \cdot (5 \cdot 7 \cdot 11) + 1 \cdot 1 \cdot (5 \cdot 6 \cdot 11) \\ &= 5643 \equiv 1023 \ \ (5 \cdot 6 \cdot 7 \cdot 11). \end{aligned}$$

Hence there are 1023 troops remaining.

2. (a) (10 points) What is the remainder when 40! is divided by 43?

Note that 43 is prime. Using Wilson's theorem we see that $42! \equiv -1 \ (43)$. This means that

$$40! \cdot 41 \cdot 42 \equiv -1 \ (43).$$

We multiply both sides by the inverse of $41 \equiv -2 \ \ (43)$, which is -22, and by the inverse of $42 \equiv -1$, which is itself. We get

$$40! \equiv -22 \equiv 21 \ \ (43).$$

So the remainder is 21.

(b) (10 points) Find the least positive residue of 2^{9202} modulo 47.

Since 47 is prime, Fermat's Little Theorem gives us $2^{46} \equiv 1 \ (47)$. Then because $9202 \equiv 2 \ (46)$, say $9202 = 46k + 2$, we see that

$$2^{9202} = (2^{46})^k \cdot 2^2 \equiv 2^2 \equiv 4 \ (47).$$

So the answer is 4.

(c) (10 points) Show that $a^6 - 1$ is divisible by 168, whenever $(a, 42) = 1$.

$168 = 2^3 \cdot 3 \cdot 7$ and $42 = 2 \cdot 3 \cdot 7$. So $(a, 168) = 1$. Further $\phi(168) = 4 \cdot 2 \cdot 6 = 48$. So Euler's theorem gives us $a^{48} \equiv 1 \ (168)$, which says $168|(a^{48} - 1)$. This is not good enough, so we need to argue differently.

Since $8, 3, 7$ are pairwise coprime and their product is 168, it suffices to show that $a^6 \equiv 1 \ (m)$ for $m = 8, 3, 7$, separately.
Since a is odd, we have (in class) $a^2 \equiv 1 \ (8)$, which implies $a^6 \equiv 1 \ (8)$.
By Fermat, we have $a^2 \equiv 1 \ (3)$, which implies $a^6 \equiv 1 \ (3)$.
Again by Fermat we have $a^6 \equiv 1 \ (7)$. Putting these together, we are done.

3. (a) (10 points) Verify that 2 is a primitive root modulo 13.

We need to show $\text{ord}_{13}2 = 12 (= \phi(13))$. By Fermat we have $2^{12} \equiv 1 \ (13)$, so (from result proved in homework), we need to check that $2^{12/p} \not\equiv 1 \ (13)$ for each prime p dividing 12. That is, we need to check $2^6 \not\equiv 1 \ (13)$ and $2^4 \not\equiv 1 \ (13)$. Both of these can be checked by calculator.

(b) (5 points) Write down all primitive roots modulo 13.

Since 2 is a primitive root, the others are of the form 2^u, where $(u, 12) = 1$. (Recalling $\phi(13) = 12$ is the order of 2, since it's a primitive root.) We find the complete list to be

$$\{2^1, 2^5, 2^7, 2^{11} \ (13)\} = \{2, 6, 11, 7 \ (13)\}.$$

4. Recall the function

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1 \\ (-1)^r, & \text{if } n \text{ is a product of } r \text{ distinct primes} \\ 0, & \text{otherwise.} \end{cases}$$

Let F denote the summatory function for μ, which is defined by $F(n) := \sum_{d|n} \mu(d)$.
(a) (5 points) Compute $F(p^k)$ for $k \geq 0$ and p a prime number.

$F(p^k) = 1$ if $k = 0$ and $F(p^k) = 0$ if $k \geq 1$.

(b) (5 points) Show that F is multiplicative. (You may quote and use the appropriate general theorem we covered in class.)

Note that F is the summatory function of μ. We know (from class) that μ is multiplicative and that the summatory function F of any multiplicative function is also multiplicative.

(c) (5 points) Using parts (a) and (b), find a simple formula for $F(n)$ (where $n \geq 1$).

$F(n) = 1$ if $n = 1$ and $F(n) = 0$ if $n > 1$.

(d) (5 points) State the Möbius inversion theorem and show how the answer to (c) is consistent with it in this case.

Möbius inversion states that if $F(n) = \sum_{d|n} f(d)$, then $f(n) = \sum_{d|n} \mu(d)F(n/d)$. Applying this to $f = \mu$, we want to check that

$$\mu(n) = \sum_{d|n} \mu(d)F(n/d).$$

But by (c), F vanishes except at 1, so the right hand side if just $\mu(n)F(n/n) = \mu(n)F(1) = \mu(n)$. This shows the answer to (c) is consistent with the inversion theorem.

5. (20 points) If the ciphertext message produced by RSA encryption with the key $(e, n) = (47, 2881)$ is 1237, what is the plaintext message? Write the answer as a block of 4 digits. Hint: $2881 = 43 \cdot 67$.

Both 43 and 67 are prime. Hence $\phi(2881) = \phi(43)\phi(67) = 42 \cdot 66 = 2772$. So the description transformation $C \mapsto C^d \ (2881)$ is given by d such that $ed = 47d \equiv 1 \ (2772)$. By the division algorithm, we find $d = 59$.

Thus we need to compute $(1237)^{59} \ (2881)$. This can be done by writing 59 in binary:

$$59 = 32 + 16 + 8 + 2 + 1$$

and then computing recursively the powers $(1237)^{2^j} \ (2881)$ for $j = 1, \ldots, 5$.

The final answer is 2012.