> *It is not knowledge, but the act of learning, not possession but the act of getting there, which grants the greatest enjoyment.*
>
> In a letter from Carl Friedrich Gauss to Farkas Bolyai (September 2nd, 1808).

Note: The final exam will be similar to the first and second prelim in format, except that the final exam will be longer (2 hours). Also, the final exam will cover all the material we have covered, with an emphasis on newer material. In order to review, you should:

1. Review the first and second midterm exams and their solutions.
2. Review the practice problems for the first and second midterm exams.
3. Review the homework assignments and their solutions.

But most importantly, study your class notes and/or the book!

Theory Question 1. Any of the theory questions in previous practice tests.

Theory Question 2. Prove the Primitive Element Theorem: Let $p > 2$ be a prime. Then $\mathbb{Z}/p\mathbb{Z}$ has a primitive root, i.e., there is a congruence $a \mod p$ of order exactly $p-1$. (You may use the theorem on the number of roots of polynomials over fields, but you certainly need to state it precisely and correctly).

Theory Question 3. Prove the following Lemma: Let p be an odd prime and let g be a primitive root modulo p. Let $a \in \mathbb{Z}$ with $(a, p) = 1$, and let n be the smallest positive integer such that $g^n \equiv a \mod p$. Then, n is even if and only if a is a quadratic residue modulo p.

Theory Question 4. Prove: if p is an odd prime, then -1 is a square mod p if and only if $p \equiv 1 \mod 4$. (You may use the previous lemma).

Theory Question 5. Write a precise statement for the Law of Quadratic Reciprocity.

Theory Question 6. Write a precise definition of the following:

1. Quadratic residue modulo m.
2. Legendre symbol.
3. Primitive root.

Question 1. 1. Find all the units in $\mathbb{Z}/28\mathbb{Z}$.

2. Find the multiplicative inverse of each unit in $\mathbb{Z}/28\mathbb{Z}$.
3. Prove that $a^{12} \equiv 1 \bmod 28$, for each unit a in $\mathbb{Z}/28\mathbb{Z}$.
4. Prove that $a^6 \equiv 1 \bmod 28$, for each unit a in $\mathbb{Z}/28\mathbb{Z}$.

Solution:
The units are those numbers between 1 and 27 that are relatively prime to $28 = 2^2 \cdot 7$. Notice that $\varphi(28) = \varphi(4)\varphi(7) = 2 \cdot 6 = 12$, so there are 12 units. Thus,

$$(\mathbb{Z}/28\mathbb{Z})^\times = \{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}.$$

Finding the multiplicative inverses is an easy calculation: for each unit u above, find another unit v in the list such that $u \cdot v \equiv 1 \bmod 28$.

Since $\varphi(28) = 12$, it follows from Euler's theorem that $a^{12} \equiv 1 \bmod 28$ for each unit a in $\mathbb{Z}/28\mathbb{Z}$. In order to prove that $a^6 \equiv 1 \bmod 28$ for each unit, we notice that $a^2 \equiv 1 \bmod 4$ by Euler's theorem ($\varphi(4) = 2$), and so $a^6 \equiv 1 \bmod 4$ as well. Moreover $a^6 \equiv 1 \bmod 7$ by Fermat's little theorem. Thus, $a^6 \equiv 1 \bmod 28$ by the Chinese remainder theorem (because 4 and 7 are relatively prime).

Question 2. Find the least non-negative residue of

$$19! + (13!)^{44} \bmod 23.$$

Explain how you calculated it and **state any theorems** you used.

Solution:
First of all, 13! is not divisible by 23 and so, by Fermat's little theorem, $(13!)^{22} \equiv 1 \bmod 23$. In particular,

$$(13!)^{44} \equiv ((13!)^{22})^2 \equiv 1^2 \equiv 1 \bmod 23.$$

Since 23 is prime, Wilson's theorem shows that $22! \equiv -1 \bmod 23$. Thus,

$$(19!) \cdot (20 \cdot 21 \cdot 22) \equiv -1 \bmod 23.$$

Since

$$-1 \equiv (19!) \cdot (20 \cdot 21 \cdot 22) \equiv 19! \cdot (-1)(-2)(-3) \bmod 23$$

it follows that $19! \equiv 6^{-1} \equiv 4 \bmod 23$. Hence

$$19! + (13!)^{44} \equiv 4 + 1 \equiv 5 \bmod 23.$$

Question 3. Let $\varphi(n)$ be the Euler "phi" function.

1. Find $\varphi(125)$. **Explain** how you did it.
2. Let $N = 3^{10!} - 1$. Is N divisible by 125? **Justify** your answer and **state** any name any theorems that you use.

Solution:
We have

$$\varphi(125) = \varphi(5^3) = 4 \cdot 5^2 = 100.$$

A number N is divisible by 125 if and only if $N \equiv 0 \bmod 125$, so we need to find the least non-negative residue of N modulo 125. Since 10! is divisible by 100 ($10! = 100 \cdot 36288$), it follows that

$$N \equiv 3^{10!} - 1 \equiv (3^{100})^{36288} - 1 \equiv 1 - 1 \equiv 0 \bmod 125,$$

where we have used Euler's theorem to prove that $3^{100} \equiv 1 \bmod 125$. Thus, N is divisible by 125.

Question 4. Find the multiplicative inverse of 113 modulo 137.

Solution:
Use Euclid's algorithm to find the GCD of 113 and 137, and then find a solution to Bezout's identity $137x + 113y = 1$. The answer is $-80 \cdot 137 + 113 \cdot 97 = 1$. Thus,

$$113^{-1} \equiv 97 \bmod 137.$$

Question 5. Find all the integral points in the line $L : 137x + 113y = 5$.

Solution:
Using Euclid's algorithm as in the previous problem, we find $-80 \cdot 137 + 113 \cdot 97 = 1$, and therefore

$$-400 \cdot 137 + 485 \cdot 113 = 5.$$

Since $\gcd(113, 137) = 1$, by a theorem we have seen, all the integral points are given by

$$\begin{cases} x = -400 + 113t, \\ y = 485 - 137t, \end{cases}$$

for any $t \in \mathbb{Z}$.

Question 6. Find all the integral points in the line $L : 185x + 111y = 7$.

Solution:
The GCD of 185 and 111 is 37, which is not a divisor of 7. Hence, this equation cannot have any integral points.

Question 7. Is 31 a quadratic residue modulo 67?

Solution:
No. We will use quadratic reciprocity. Note that $67 \equiv 31 \equiv 3 \bmod 4$, and 31 and 67 are primes:

$$\left(\frac{31}{67}\right) = -\left(\frac{67}{31}\right) = -\left(\frac{5}{31}\right) = -\left(\frac{31}{5}\right) = -\left(\frac{1}{5}\right) = -1.$$

Question 8. Show that the hyperbola $C : x^2 - 67y^2 = 31$ has no integral points.

Solution:
Suppose it has an integral point $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$. Then

$$x_0^2 - 67y_0^2 = 31$$

and reducing modulo 67 we obtain $x_0^2 \equiv 31 \bmod 67$. But 31 is a unit, and a quadratic non-residue by the previous problem, so this congruence has no solutions. We have reached a contradiction.

Question 9. Let g be a primitive root modulo 29.

1. How many primitive roots are there modulo 29?
2. Find a primitive root g modulo 29.
3. Use g mod 29 to find **all** the primitive roots modulo 29.
4. Use the primitive root g mod 29 to express all the quadratic residues modulo 29 as powers of g.
5. Find all the quadratic residues modulo 29, and all the quadratic non-residues modulo 29.
6. Is 5 a quadratic residue modulo 29? If so, is 5 congruent to a fourth power modulo 29?
7. Use the primitive root g mod 29 to calculate all the congruence classes that are congruent to a fourth power.
8. Show that the equation $x^4 - 29y^4 = 5$ has no integral solutions.

Solution:

1. By our results on primitive roots, and since 29 is prime, there is at least one primitive root, and in fact there are
$$\varphi(\varphi(29)) = \varphi(28) = 12$$
primitive roots.
2. The number 2 is a primitive root modulo 29. (Verify this.)
3. The primitive roots are the powers 2^n mod 29 such that $\gcd(n, 28) = 1$, i.e.,
$$\{2^n : n = 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\},$$
so the primitive roots are $2, 8, 3, 19, 18, 14, 27, 21, 26, 10, 11, 15$.
4. Given a primitive root g mod p, the quadratic residues are the even powers of g.
5. Thus, the quadratic residues are 2^{2n} for $n = 1, \ldots, 14$,
$$4, 16, 6, 24, 9, 7, 28, 25, 13, 23, 5, 20, 22, 1$$
and the quadratic non-residues are 2^{2n+1} for $n = 0, \ldots, 13$, i.e.,
$$2, 8, 3, 12, 19, 18, 14, 27, 21, 26, 17, 10, 11, 15.$$
6. Yes, 5 is a QR, see list above. By taking the 4th power of every unit (between 1 and 14) we obtain the list of all possible 4th powers modulo 29:
$$1, 16, 23, 24, 16, 20, 23, 7, 7, 24, 25, 1, 25, 20$$
or $1, 7, 16, 20, 23, 24, 25$ mod 29. Hence 5 is not a fourth power.
7. One can come up with the same list by calculating all the powers of 2 mod 29 that are divisible by 4, i.e., 2^{4n} with $n = 0, \ldots, 7$:
$$1, 16, 24, 7, 25, 23, 20, 1.$$
8. Suppose that $x^4 - 29y^4 = 5$ has an integral solution $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$. Then, reducing modulo 29 we obtain
$$x_0^4 \equiv 5 \bmod 29$$
but 5 is not a fourth power, so this is impossible.