Math 445. Final Exam

(1) Definitions/Theorem statements

(a) State **Fermat's little theorem**.

If p is an odd prime and a is not a multiple of p, then $a^{p-1} \equiv 1 \pmod{p}$.

(b) Define the **order** of an element in a group.

Let G be a group with identity element 1. The order of an element g in a group G is the least positive integer n such that $g^n = 1$, if such an n exists, and ∞ if no such n exists.

(c) State **Euler's criterion**.

If p is an odd prime and a is not a multiple of n, then $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

(d) State the **Dirichlet's approximation theorem**.

For any irrational number α, there are infinitely many rational numbers $\frac{p_k}{q_k}$ such that $\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k^2}$.

(2) Computations.

(a) Compute the inverse of $[311]_{3141}$.

From the Euclidean algorithm, we have

$$\begin{aligned} 3141 &= 10 \cdot 311 + 31 \\ 311 &= 10 \cdot 31 + 1 \\ 1 &= 1 \cdot 311 - 10 \cdot 31 \\ &= 1 \cdot 311 - 10(1 \cdot 3141 - 10 \cdot 311) \\ &= -10 \cdot 3141 + 101 \cdot 311 \end{aligned}$$

so $[101]_{3141}$ is the inverse.

(b) On the real elliptic curve $\overline{E}$ given by the equation $y^2 = x^3 + 12x + 9$ with group operation $\star$, compute $(0,3) \star (0,3)$.

To double a point on an elliptic curve, we compute the tangent line and find the third point on the line. We have $2y\,y' = 3x^2 + 12$, so y' at $(0,3)$ is $12/6 = 2$; thus, the tangent line is $y = 2(x-0)+3 = 2x+3$. Substituting into the equation of the curve, we get

$$(2x+3)^2 = x^3 + 12x + 9 \quad \rightsquigarrow \quad x^3 - 4x^2 = 0$$

so $x = 4$ and $y = 11$. The group operation then requires reflection over the x-axis, so the desired point is $(4, -11)$.

(c) Determine whether 67 is a square modulo 221. Note that 67 and 221 are prime. If any step in your calculation has a congruence condition as a hypothesis, be sure to indicate it.

$$\begin{aligned}
\left(\frac{67}{221}\right) &= -\left(\frac{221}{67}\right) && \text{since } 221 \equiv 67 \equiv 3 \pmod 4 \\
&= -\left(\frac{10}{67}\right) && \text{since } 221 \equiv 10 \pmod{67} \\
&= -\left(\frac{5}{67}\right)\left(\frac{2}{67}\right) \\
&= -\left(\frac{5}{67}\right)\cdot(-1) = \left(\frac{5}{63}\right) && \text{since } 67 \equiv \pm 3 \pmod 8 \\
&= \left(\frac{67}{5}\right) && \text{since } 5 \equiv 1 \pmod 4 \\
&= \left(\frac{2}{5}\right) && \text{since } 67 \equiv 2 \pmod 5 \\
&= -1
\end{aligned}$$

so 67 is not a square modulo 221.

(d) Find the first two convergents (*after* $C_0 = \frac{5}{1}$) in the continued fraction expansion of $\sqrt{29}$ and use a result from class to bound $|C_2 - \sqrt{29}|$.

To compute the continued fraction we have

$$\sqrt{29} = 5 + (\sqrt{29} - 5) = 5 + \frac{1}{\left(\frac{1}{\sqrt{29}-5}\right)} = 5 + \frac{1}{\left(\frac{\sqrt{29}+5}{4}\right)} = 5 + \frac{1}{2 + \frac{\sqrt{29}-3}{4}}$$

$$= 5 + \frac{1}{2 + \frac{1}{\left(\frac{4}{\sqrt{29}-3}\right)}} = 5 + \frac{1}{2 + \frac{1}{\left(\frac{\sqrt{29}+3}{5}\right)}} = 5 + \frac{1}{2 + \frac{1}{1+\ddots}}$$

so $C_1 = 5 + \frac{1}{2} = \frac{11}{2}$ and $C_2 = 5 + \frac{1}{2+\frac{1}{1}} = \frac{16}{3}$.

By our Theorem about convergents and good approximations, we have $\left|\sqrt{29} - \frac{16}{3}\right| < \frac{1}{9}$.

(e) One integer solution of the equation $x^2 - 30y^2 = 1$ is given by $(x, y) = (11, 2)$. Find two other pairs of positive integers (x, y) that are solutions of the given equation.

Note that the given solution is the smallest positive solution, since $y = 1$ yields $x^2 = 31$ which has no solution x. Then by the general theory, we know that every solution is given by $(\pm x, \pm y)$ where $x + y\sqrt{30} = (11 + 2\sqrt{30})^k$ for some k. Taking $k = 2, 3$ we get the solutions

$$(11 + 2\sqrt{30})^2 = 241 + 44\sqrt{30} \rightsquigarrow (241, 44)$$
$$(11 + 2\sqrt{30})^3 = 5291 + 966\sqrt{30} \rightsquigarrow (5291, 966)$$

(f) Solve $x^{187} \equiv 103 \pmod{319}$. Note that $319 = 11 \cdot 29$.

First, we compute $\varphi(319) = 11 \cdot 28 = 280$. Then we can use the Euclidean algorithm to find the inverse of 187 modulo 280:

$$\begin{aligned} 280 &= 1 \cdot 187 + 93 \\ 187 &= 2 \cdot 93 + 1 \\ 1 &= 1 \cdot 187 - 2 \cdot 93 \\ &= 1 \cdot 187 - 2(1 \cdot 280 - 1 \cdot 187) \\ &= -2 \cdot 280 + 3 \cdot 187 \end{aligned}$$

so the inverse is $[3]$. Then, since $3 \cdot 187 = 280k + 1$

$$x \equiv x^{280k+1} \equiv x^{3 \cdot 187} \equiv (x^{187})^3 \equiv 103^3 \equiv 152 \pmod{319}.$$

(3) Proofs. Choose **three** of the problems in this part. If you write in more than three answer areas, be sure to make clear which three you would like to be graded.

(a) Let $\gcd(a, 101) = 1$.

(i) Show that if a has a fourth root modulo 101, then $a^{25} \equiv 1 \pmod{101}$.

(ii) Show[1] that if $a^{25} \equiv 1 \pmod{101}$, then a has a fourth root modulo 101.

(i) If a has b as a fourth root, then $a \equiv b^4 \pmod{101}$, and then $a^25 \equiv (b^4)^{25} = b^{100} \equiv 1 \pmod{101}$ by Fermat's Little Theorem.

(ii) Let g be a primitive root modulo 101. We can write $a = g^s = g^{4k+r}$ for some $r = 0, 1, 2, 3$. If $a^{25} \equiv 1 \pmod{101}$, then

$$1 \equiv (g^{4k+r})^{25} \equiv g^{100k+25r} \equiv g^{25r}$$

by Fermat again. But $25r < 100$ so since g is a primitive root, we must have $r = 0$. Thus, $a = g^{4k} = (g^k)^4$, so a has a fourth root.

[1] Hint: Write $a = g^{4k+r}$ for some primitive root g.

(b) Consider the equation $y^2 = x^3 + ax + b$ where $a, b \in \mathbb{Z}$ are integers with $4a^3 \neq 27b^2$ (this is the technical condition on coefficients for an elliptic curve). Suppose that there are exactly 15 pairs of rational numbers (x, y) are solutions to this equation. Prove that this curve does *not* have any rational inflection points.

The set of rational points plus "∞" forms a group, which has 16 elements. If there was a rational inflection point, it would be an element of this group with order three. But the order of an element divides the order of the group by Lagrange, so this is impossible.

(c) Modify Euclid's argument to show that there are infinitely many primes p such that $p \equiv 3 \pmod 4$.

By way of contradiction, suppose that there are only finitely many primes $p_1, \ldots, p_k$ that are congruent to $3 \pmod 4$. Consider the number $N = 4p_1p_2 \cdots p_k - 1$.
We claim that N is divisible by some prime that is congruent to 3 modulo 4. Since N is odd, it is a product of odd primes; in particular, each prime factor is congruent to 1 or 3 modulo 4. If each factor is congruent to 1, then their product is congruent to 1, but $N \equiv 3 \pmod 4$. Thus, N is divisible by some prime that is congruent to 3 modulo 4.
Thus, N is divisible by p_i for some i. But $N \equiv -1 \pmod{p_i}$, so N is not a multiple of p_i. This is a contradiction. We conclude that there must be infinitely many primes that are congruent to 3 modulo 4.

(d) Show that[2] there is no element of order 24 in $\mathbb{Z}_{52}^{\times}$.

We will show that if $\gcd(a, 52) = 1$, then a satisfies $a^{12} \equiv 1 \pmod{52}$. By CRT, this is equivalent to

$$\begin{cases} a^{12} \equiv 1 \pmod{4} \\ a^{12} \equiv 1 \pmod{13} \end{cases}$$

Note that $\gcd(a, 4) = 1$ and $\gcd(a, 13) = 1$. Thus, by FLT, we have

$$a^{12} \equiv 1 \pmod{13}.$$

If $\gcd(a, 4) = 1$, then $a \equiv 1, 3 \pmod{4}$, so $a^2 \equiv 1 \pmod{4}$, and $a^{12} = (a^2)^6 \equiv 1 \pmod{4}$ too. Thus $a^{12} \equiv 1 \pmod{52}$ as claimed.
By definition of order, the order of $[a]_{52}$ is at most 12; in particular, it cannot be 24.

[2] Hint: Show that every element satisfies $x^{12} \equiv 1$ instead, perhaps with the help of CRT...

(e) Show that the equation $x^2 + 2x + y^2 = 4202$ has no integer solutions x, y.

We consider this equation modulo 4: this reduces to $x^2 + 2x + y^2 \equiv 1 \pmod 4$. Plugging in $x \equiv 0, 1, 2, 3 \pmod 4$ we get $x^2 + 2x \equiv 0, 3, 0, 3 \pmod 4$ and plugging in $y \equiv 0, 1, 2, 3 \pmod 4$ we get $y^2 \equiv 0, 1, 0, 1 \pmod 4$. Thus, the left hand side can only take values $\equiv 0 + 0, 0 + 1, 3 + 0, 3 + 1 \equiv 0, 1, 3, 0 \pmod 4$. Since the right hand side is congruent to $2 \pmod 4$, there is no solution.

Bonus: On the first week of class, we considered some examples of Pythagorean triples where the lengths of the legs were nearly equal. Let's say that a right triangle with integer side lengths is **almost isoceles** if the lengths of its two legs[3] differ by one; for example, the triangle with lengths $3, 4, 5$ and the triangle with lengths $20, 21, 29$ are almost isoceles.

Find a recipe for infinitely many such triangles, and use it to write down three more besides the examples above.

We can write $b = a + 1$. Then, from the Pythagorean theorem, we are looking for pairs of positive integers (a, c) such that $a^2 + (a+1)^2 = c^2$. We can rewrite this as

$$2a^2 + 2a + 1 = c^2$$
$$4a^2 + 4a + 1 + 1 = 2c^2$$
$$(2a+1)^2 - 2c^2 = -1.$$

Writing $x = 2a + 1$ and $y = c$, we get

$$x^2 - 2y^2 = -1.$$

The smallest solution to this equation is $(x, y) = (1, 1)$. We know that if (u, v) is a solution to the equation

$$x^2 - 2y^2 = 1$$

then $N((u + v\sqrt{2})(1 + \sqrt{2})) = N((u + v\sqrt{2}))N((1 + \sqrt{2})) = 1(-1) = -1$, so the coefficients of $(u + v\sqrt{2})(1 + \sqrt{2})$ form another solution. The solutions of $x^2 - 2y^2 = 1$ are given by (u_k, v_k) where

$$u_k + v_k\sqrt{2} = (3 + 2\sqrt{2})^k,$$

so we get solutions (x_k, y_k) where

$$x_k + y_k\sqrt{2} = (1 + \sqrt{2})(3 + 2\sqrt{2})^k,$$

As long as x_k is odd, every such solution yields a solution $(a, c) = (\frac{x_k - 1}{2}, y_k)$ to $a^2 + (a + 1)^2 = c^2$, and thus $(a, a + 1, c)$ as a triple of side lengths of an almost isosceles triangle.

Taking $k = 1, 2, 3, 4, 5$, we obtain $(3, 4, 5)$, $(20, 21, 29)$, $(119, 120, 169)$, $(696, 697, 985)$, $(4059, 4060, 5741)$.

[3] Note: legs, not leg and hypotenuse.