Math 445. Exam #1

(1) Definitions/Theorem statements

(a) State the definition of a **Pythagorean triple**.

A triple of integers (a, b, c) is a Pythagorean triple if they form the side lengths of a right triangle.

OR

A triple of integers (a, b, c) is a Pythagorean triple if $a^2 + b^2 = c^2$.

(b) State **Fermat's Little Theorem**.

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

(c) State the definition of a **primitive root**.

An element of $\mathbb{Z}_n^\times$ is a primitive root if its order equals $\varphi(n)$.

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

For p an odd prime and a coprime to p, $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

(2) Computations.

(a) • Use the definition of congruence to verify that

$$\begin{cases} 54 \equiv 10 \pmod{11} \\ 54 \equiv 3 \pmod{17} \end{cases}$$

$$54 - 10 = 44 = 4 \cdot 11 \qquad 54 - 3 = 51 = 3 \cdot 17.$$

• Explicitly describe the set of integers x that satisfies the two congruences

$$\begin{cases} x \equiv 10 \pmod{11} \\ x \equiv 3 \pmod{17} \end{cases}$$

$$\{54 + 187k \mid k \in \mathbb{Z}\}$$

(b) Find the inverse of $[121]$ in $\mathbb{Z}_{369}$.

We use the Euclidean algorithm:

$$\begin{aligned} 369 &= 3 \cdot 121 + 6 \\ 121 &= 20 \cdot 6 + 1 \\ 1 &= 1 \cdot 121 - 20 \cdot 6 \\ &= 1 \cdot 121 - 20(1 \cdot 369 - 3 \cdot 121) \\ &= 61 \cdot 121 - 20 \cdot 369. \end{aligned}$$

Thus $61 \cdot 121 \equiv 1 \pmod{369}$, so $[61]$ is the inverse.

(c) Determine if 83 is a quadratic residue modulo 97. (Both 83 and 97 are primes; you do not need to check this.)

We apply quadratic reciprocity and its variants:

$$\left(\frac{83}{97}\right) = \left(\frac{97}{83}\right) = \left(\frac{14}{83}\right) = \left(\frac{2}{83}\right)\left(\frac{7}{83}\right)$$
$$= -1 \cdot -\left(\frac{83}{7}\right) = -1 \cdot -\left(\frac{6}{7}\right) = -1 \cdot -1 = 1$$

so this is a quadratic residue.

(d) Find the smallest nonnegative integer n such that $17^{3202} \equiv n \pmod{250}$.

We apply Euler's theorem. First we compute

$$\varphi(250) = \varphi(2^1 \cdot 5^3) = (5-1)5^2 = 100.$$

Then $17^{100} \equiv 1 \pmod{250}$ by Euler, so

$$17^{3202} = 17^{32 \cdot 100 + 2} \equiv 17^2 \equiv 289 \equiv 39 \pmod{250}.$$

So, we get 39.

(3) Proofs.

(a) Without using the Sums of Two Squares Theorem, show there are no integers a, b, c such that $a^2 + b^2 + 1 = (2c)^2$.

We consider this equation modulo 4. We know that a^2 is equivalent to 0 or 1 modulo 4, and likewise with b^2 and c^2. Then since $0 \cdot 2^2$ and $1 \cdot 2^2$ are both equivalent to 0 modulo 4 and $(2c)^2 \equiv 0 \pmod 4$. Considering the cases for a, b, the left hand side is either $1, 2$, or 3 modulo 4, so there cannot be any solution.

(b) Let p, q be distinct primes and $a \in \mathbb{Z}$. Show that $[a]_{pq}$ has at most four square roots in $\mathbb{Z}_{pq}$. (Hint: Show that if $b^2 \equiv a \pmod{pq}$, then $b^2 \equiv a \pmod{p}$ and $b^2 \equiv a \pmod{q}$.)

Let $[b]_{pq}$ be a square root of $[a]_{pq}$, so $b^2 \equiv a \pmod{pq}$. Show that $b^2 \equiv a \pmod{p}$ and $b^2 \equiv a \pmod{q}$, since $p|(pq)$ and $q|(pq)$. From the first equation, we know that there is some $[c]_p$ such that $[b]_p = \pm[c]_p$ and there is some $[d]_q$ such that $[b]_q = \pm[d]_q$.
For each of the four possibilities $([c], [d])$, $(-[c], [d])$, $([c], -[d])$, $(-[c], -[d])$, there is a unique congruence class in $\mathbb{Z}_{pq}$ that corresponds to both equivalences mod p and mod q by the uniqueness part of CRT. Thus, there are at more four square roots for $[a]$.

(c) Let p be an odd prime such that $p \equiv 2 \pmod 3$. Show that every element of $\mathbb{Z}_p^\times$ has a cube root; i.e., if $a \in \mathbb{Z}_p^\times$, there is some $b \in \mathbb{Z}_p^\times$ such that $b^3 = a$.

Let g be a primitive root and write $a = g^k$. We seek an element $b = g^\ell$ such that $b^3 = a$; i.e., $g^{3\ell} = g^k$. Since $g^{p-1} = [1]$ in $\mathbb{Z}_p$, we have

$$g^{3\ell} = g^k$$

whenever

$$3\ell \equiv k \pmod{p-1}.$$

But, since

$$p \equiv 2 \pmod 3,$$

we also have

$$p - 1 \equiv 1 \pmod 3,$$

which implies that 3 and $p-1$ are coprime; i.e., 3 is a unit modulo $p-1$, so

$$3\ell \equiv k \pmod{p-1}$$

has a solution ℓ; this yields the cube root $b = g^\ell$ that we seek.

Bonus: Let p be an odd prime such that $p \equiv 1 \pmod 3$. Show that $a \in \mathbb{Z}_p^\times$ has a cube root if and only if $a^{(p-1)/3} = [1]$.

For the forward direction, if $a = b^3$, then $a^{(p-1)/3} = b^{3(p-1)/3} = b^{p-1} = [1]$ by Fermat's little Theorem.

For the reverse implication, write $a = g^k$ for a primitive root g. Then

$$[1] = a^{(p-1)/3} \equiv g^{(p-1)k/3}$$

implies that $(p-1)k/3$ is a multiple of $p-1$, by definition of primitive root. Thus we can write $k = 3\ell$ for some ℓ. Then $a = g^{3\ell} = (g^\ell)^3$ is a cube.

Bonus: Characterize all rational numbers r such that the circle $x^2+y^2=r$ has a rational point.

Suppose that $x = a/b$, $y = c/d$, and $r = \frac{s}{t}$ are rational numbers in lowest terms such that $x^2 + y^2 = r$, so

$$\frac{s}{t} = \frac{a^2}{b^2} + \frac{c^2}{d^2} = \frac{(ad)^2 + (bc)^2}{(bd)^2},$$

and

$$s(bd)^2 = ((ad)^2 + (bc)^2)t.$$

By sums of two squares, we know that for each prime $q \equiv 3 \pmod 4$, we have that the multiplicity of q in $(ad)^2 + (bc)^2$ is even. Likewise, the multiplicity of q in $(bd)^2$ is even. This implies that if q divides s, its multiplicity in s is even, or if q divides t, its multiplicity in t is even. That means we can write

$$r = 2^a p_1^{e_1} \cdots p_k^{e_k} q_1^{2f_1} \cdots q_\ell^{2f_\ell}$$

with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$, and $a, e_i, f_j \in \mathbb{Z}$.

We claim that every rational number of this form can be written as a sum of two rational squares. Take

$$r = 2^a p_1^{e_1} \cdots p_k^{e_k} q_1^{2f_1} \cdots q_\ell^{2f_\ell}$$

and write $r = s/t$ in lowest terms by collecting the positive exponents into s and the negative exponents into t.

By adding redundant factors of 2 and p_i to s and t if necessary (but not any additional q_j factors) we can assume that $t = w^2$ is a perfect square, and that the multiplicity of each q_j in s is still even. Therefore, $s = u^2 + v^2$ is a sum of squares, so

$$\frac{s}{t} = \left(\frac{u}{w}\right)^2 + \left(\frac{v}{w}\right)^2.$$

That is, the circle with radius r has a rational point.