M328K: Homework 9

Katherine Ho

November 20, 2024

1. Let p be an odd prime with $p \equiv 5 \pmod 8$. Find an explicit solution to the congruence $x^2 \equiv -1 \pmod p$. (Hint: You know $(2/p) = -1$. Apply Euler's criterion.)

   Proof. Given $p \equiv 5 \pmod 8$, we know that $\left(\frac{2}{p}\right) = -1$. By Euler's Criterion,

   $$2^{\frac{p-1}{2}} \equiv -1 \pmod p$$

   Consider $x = 2^{\frac{p-1}{4}}$. From the above property we have

   $$x^2 = 2^{\frac{p-1}{4}^2} \equiv 2^{\frac{p-1}{2}} \equiv -1$$

   Thus an explicit solution to $x^2 \equiv -1 \pmod p$ is $x = 2^{\frac{p-1}{4}}$. $\square$

2. (a) Use the previous problem to find a solution x to the congruence $x^2 \equiv -1 \pmod{541}$. (Reduce modulo p so that $0 < x < 541$)

   Proof. From the previous problem, $x = 2^{\frac{541-1}{4}} = 2^{135}$. Using binomial expansion:

   $$2^{135} = 2^{128} \cdot 2^4 \cdot 2^2 \cdot 2^1$$

   $$\begin{aligned}
   2^1 &\equiv 2 \pmod{541}\\
   2^2 &\equiv 4 \pmod{541}\\
   2^4 &\equiv 16 \pmod{541}\\
   2^8 &\equiv 256 \pmod{541}\\
   2^{16} &\equiv 75 \pmod{541}\\
   2^{32} &\equiv 215 \pmod{541}\\
   2^{64} &\equiv 240 \pmod{541}\\
   2^{128} &\equiv 254 \pmod{541}
   \end{aligned}$$

   By substitution,

   $$2^{135} = 254 \cdot 16 \cdot 4 \cdot 2 \equiv 32512 \equiv 52 \pmod{541}$$

   Thus $x \equiv 52 \pmod{541}$. $\square$

(b) Use part (a) to express a multiple of 541 as a sum of squares.

Proof. We can substitute $x \equiv 52 \pmod{541}$ into $x^2 \equiv -1 \pmod{541}$.

$$52^2 \equiv -1 \pmod{541}$$

By the definition of congruence,

$$52^2 + 1^2 = 541 \cdot k \quad \text{for some } k \in \mathbb{Z}$$

Thus a multiple of 541 can be expressed as a sum of squares. □

(c) Use Fermat's method of descent to express 541 as a sum of squares.

Proof. Since $541 \equiv 1 \pmod{4}$, then

$$\left(\frac{-1}{541}\right) = 1 \to x^2 + 1 = k \cdot 541 \to x = 52, k = 5$$

Suppose

$$52^2 + 1^2 = 5 \cdot 541$$

Then find u, v such that

$$\begin{aligned} u &\equiv 52 \pmod{5} \to u = 2 \\ v &\equiv 1 \pmod{5} \to v = 1 \end{aligned}$$

Thus

$$\to 52^2 + 1^2 \equiv 2^2 + 1^2 \equiv 0 \pmod{5}$$

Then,

$$\begin{aligned} (52^2 + 1^2)(2^2 + 1^2) &= 5^2 \cdot 1 \cdot 541 \\ (2 \cdot 52 + 1 \cdot 1)^2 + (52 - 2(1))^2 &= 5^2 \cdot 541 \\ 2(52) + (1) \equiv 52^2 + 1^2 \equiv 52^2 \cdot 1^2 &\equiv 0 \pmod{5} \\ 52 - 2 \cdot 1 \equiv 52 - 52 &\equiv 0 \pmod{5} \\ (\frac{2(52)+1}{5})^2 + (\frac{52 - 2(1)}{5})^2 &= 541 \end{aligned}$$

$$\boxed{21^2 + 10^2 = 541}$$

□

3. Let $\alpha = a + bi$ be a Gaussian integer. Show that if $N(\alpha) = a^2 + b^2$ is divisible by an odd prime p with $p \equiv 3 \pmod{4}$, then both a and b are divisible by p.

(Hint: By contradiction, assume a and b are not divisible by p. Then the Legendre symbols $\left(\frac{a}{p}\right)$ and $\left(\frac{b}{p}\right)$ are well-defined. Now derive a contradiction.)

Proof. Assume a and b are both not divisible by p. Then the Legendre symbols $\left(\frac{a}{p}\right)$ and $\left(\frac{b}{p}\right)$ are well-defined.

Since $N(\alpha) = a^2 + b^2$ is divisible by p, then

$$a^2 + b^2 \equiv 0 \pmod{p}$$

Then

$$a^2 \equiv -b^2 \pmod{p}$$

Taking the Legendre symbol of both sides, we have

$$\left(\frac{a^2}{p}\right) = \left(\frac{-b^2}{p}\right)$$

We see that a^2 is a QR of p so $\left(\frac{a^2}{p}\right) = 1$.

And,

$$\left(\frac{-b^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{-1}{p}\right) \cdot 1 = \left(\frac{-1}{p}\right) = -1$$

By substitution:

$$\left(\frac{a^2}{p}\right) = \left(\frac{-b^2}{p}\right) \to 1 = -1$$

This is a contradiction. Hence if $N(\alpha) = a^2 + b^2$ is divisible by an odd prime p with $p \equiv 3 \pmod{4}$, then both a and b are divisible by p.

□

4. Show how to factor 27007 if you know both 885 and 7816 are square roots of 22 modulo 27007.

Proof. If 885 and 7816 are square roots of 22 modulo 27007, then

$$\begin{aligned} 885^2 &\equiv 7816^2 \pmod{27007} \\ 27007 &\mid (885^2 - 7816^2) \\ 27007 &\mid (885 + 7816)(885 - 7816) \end{aligned}$$

We can use this to find the factors of 27007.

$$\begin{aligned} 885 + 7816 &\equiv 8701 \pmod{27007} \\ 885 - 7816 &\equiv -6931 \equiv 20076 \pmod{27007} \end{aligned}$$

Then find $\gcd(8701, 27007)$ and $\gcd(20076, 27007)$ to get the factors.

$$\begin{aligned} 27007 &= 8701 * 3 + 904 \\ 8701 &= 904 * 9 + 565 \\ 904 &= 565 * 1 + 339 \\ 565 &= 339 * 1 + 226 \\ 339 &= 226 * 1 + 113 \\ 226 &= 113 * 2 + 0 \end{aligned}$$

$gcd(8701, 27007) = 113$.

$$\begin{aligned}
27007 &= 20076 * 1 + 6931 \\
20076 &= 6931 * 2 + 6214 \\
6931 &= 6214 * 1 + 717 \\
6214 &= 717 * 8 + 478 \\
717 &= 478 * 1 + 239 \\
478 &= 239 * 2 + 0
\end{aligned}$$

$\gcd(20076, 27007) = 239$.

Thus $27007 = 113 \cdot 239$. □

5. Find the four incongruent solutions of the quadratic congruence $x^2 \equiv 30 \pmod{133}$.

Proof. 133 can be factored as $7 * 19$. Then we can solve

$$x^2 \equiv 30 \pmod 7 \quad \text{and} \quad x^2 \equiv 30 \pmod{19}$$

$$\begin{aligned}
x^2 &\equiv 30 \pmod 7 \\
x^2 &\equiv 2 \pmod 7 \\
x &\equiv \pm 3 \pmod 7
\end{aligned}$$

$$\begin{aligned}
x^2 &\equiv 30 \pmod{19} \\
x^2 &\equiv 11 \pmod{19} \\
x &\equiv \pm 7 \pmod{19}
\end{aligned}$$

Now we can look at these four cases and solve with the Chinese Remainder Theorem:

- $x \equiv 3 \pmod 7, \quad x \equiv 7 \pmod{19} \quad \to x \equiv 45 \pmod{133}$
- $x \equiv -3 \pmod 7, \quad x \equiv 7 \pmod{19} \quad \to x \equiv 102 \pmod{133}$
- $x \equiv 3 \pmod 7, \quad x \equiv -7 \pmod{19} \quad \to x \equiv 31 \pmod{133}$
- $x \equiv -3 \pmod 7, \quad x \equiv -7 \pmod{19} \quad \to x \equiv 88 \pmod{133}$

Thus the four incongruent solutions are $x \equiv 31, 45, 88, 102$. □

6. We have seen that any prime of the form $p = 4k + 1$ can be expressed as a sum of two squares. Prove that this representation is unique (except for swapping the order of the two summands).

(Hint: Suppose that $p = a^2 + b^2 = c^2 + d^2$, where a, b, c, d are all positive integers. First argue that $a^2d^2 \equiv b^2c^2 \pmod p$, so then $ad \equiv bc \pmod p$ or $ad \equiv -bc \pmod p$. Next, argue that these two cases imply, respectively, that $ad - bc = 0$ or $ad + bc = p$. If $ad + bc = p$, use the product formula to write p^2 as a sum of squares and then use the resulting equation to conclude $ac - bd = 0$. Thus, it follows that either $ad = bc$ or $ac = bd$. Now draw the rest of the owl.)

Proof. Suppose this representation is not unique; that is $p = a^2 + b^2 = c^2 + d^2$, where a, b, c, d are all positive integers.

$$\begin{aligned} p &= a^2 + b^2 \\ pd^2 &= d^2(a^2 + b^2) \\ p &= c^2 + d^2 \\ pb^2 &= b^2(c^2 + d^2) \end{aligned}$$

Subtracting these two equations, we get

$$\begin{aligned} pd^2 - pb^2 &= d^2(a^2 + b^2) - b^2(c^2 + d^2) \\ p(d^2 - b^2) &= a^2d^2 - b^2c^2 \end{aligned}$$

Thus $a^2d^2 \equiv b^2c^2 \pmod{p}$. Taking the square root of both sides, we get

$$ad \equiv bc \pmod{p} \quad \text{or} \quad ad \equiv -bc \pmod{p}$$

Case 1: $ad \equiv bc \pmod{p}$.

$$\begin{aligned} ad &\equiv bc \pmod{p} \\ ad - bc &\equiv 0 \pmod{p} \\ ad - bc &= p \cdot x \end{aligned}$$

In this case, $ad - bc$ must be 0.

Case 2: $ad \equiv -bc \pmod{p}$

$$\begin{aligned} ad &\equiv -bc \pmod{p} \\ ad + bc &\equiv 0 \pmod{p} \\ ad + bc &= p \cdot x \end{aligned}$$

Since $a, b, c, d < p$, then $ad + bc = p$.

If $ad + bc = p$, by the product formula we have

$$\begin{aligned} p^2 &= (ad + bc)(ad + bc) \\ &= a^2d^2 + 2abcd + b^2c^2 \end{aligned}$$

From this we see that $ac - bd = 0$.

Now we know that $ad = bc$ or $ac = bd$.

Since $a \neq b$, then this can only be true for $a = d$ and $b = c$. Thus $p = a^2 + b^2$, that is, there is a unique sum of 2 squares for any prime. $\square$