

SOLUTIONS TO HOMEWORK 4
Math 104 - Dr. Evans
UCSD Winter 2004

1. (a) Use Euclidean algorithm to find integers x and y such that $101x + 191y = 1$.
(b) Use the solution from part (a) to find an inverse of 101 modulo 191. Make your answer between 0 and 190.

(a) Using the Euclidean algorithm results in the following set of equations:

$$\begin{array}{ll} 191 = 1 \cdot 101 + 90 & 90 = 191 - 101 \\ 101 = 1 \cdot 90 + 11 & 11 = 101 - 90 \\ 90 = 8 \cdot 11 + 2 & 2 = 90 - 8 \cdot 11 \\ 11 = 5 \cdot 2 + 1 & 1 = 11 - 5 \cdot 2 \\ 2 = 2 \cdot 1 + 0 & \end{array}$$

Starting from the bottom equation on the right side and substituting, we have

$$\begin{aligned} 1 &= 11 - 5 \cdot 2 \\ &= 11 - 5(90 - 8 \cdot 11) \\ &= 41 \cdot 11 - 5 \cdot 90 \\ &= 41(101 - 90) - 5 \cdot 90 \\ &= 41 \cdot 101 - 46 \cdot 90 \\ &= 41 \cdot 101 - 46(191 - 101) \\ &= 87 \cdot 101 - 46 \cdot 191 \end{aligned}$$

Hence, $x = 87$ and $y = -46$ are integers such that $101x + 191y = 1$.

(b) Since $1 = 87 \cdot 101 - 46 \cdot 191$, then $1 \equiv 87 \cdot 101 \pmod{191}$. By the definition of inverse modulo 191, 87 is the inverse of 101 modulo 191.

2. Prove that for any two positive integers a and m , a has an inverse modulo m if and only if $\gcd(a, m) = 1$.

Suppose that a has an inverse modulo m . Then there exists an integer x such that $ax \equiv 1 \pmod{m}$. By definition, there exists an integer y such that $ax = 1 + my$, or equivalently, $ax - my = 1$. Since $\gcd(a, m) | a$ and $\gcd(a, m) | m$, we also have $\gcd(a, m) | ax - my = 1$. Hence, $\gcd(a, m) = 1$.

Now suppose that $\gcd(a, m) = 1$. By the Euclidean algorithm, we can find integers x and y such that $ax + my = 1$. Reducing modulo m results in $ax \equiv 1 \pmod{m}$. Therefore, x is an inverse of a modulo m , which shows that a has an inverse modulo m .

3. A quadratic residue for an odd prime p is a number b between 1 and $p - 1$ such that $x^2 \equiv b \pmod{p}$ has a solution. Find the quadratic residues for $p = 19$ and $p = 23$. In general, how many quadratic residues do you think there are for any odd prime p ?

From class, it is enough to find the squares of $x = 1, 2, \dots, \frac{p-1}{2}$. So we start with $p = 19$:

$$\begin{array}{lll} 1^2 \equiv 1 \pmod{19} & 4^2 \equiv 16 \pmod{19} & 7^2 \equiv 11 \pmod{19} \\ 2^2 \equiv 4 \pmod{19} & 5^2 \equiv 6 \pmod{19} & 8^2 \equiv 7 \pmod{19} \\ 3^2 \equiv 9 \pmod{19} & 6^2 \equiv 17 \pmod{19} & 9^2 \equiv 5 \pmod{19} \end{array}$$

The quadratic residues of $p = 19$ are $\{1, 4, 5, 6, 7, 9, 11, 16, 17\}$.

Now we do the same with $p = 23$:

$$\begin{array}{lll} 1^2 \equiv 1 \pmod{23} & 5^2 \equiv 2 \pmod{23} & 9^2 \equiv 12 \pmod{23} \\ 2^2 \equiv 4 \pmod{23} & 6^2 \equiv 13 \pmod{23} & 10^2 \equiv 8 \pmod{23} \\ 3^2 \equiv 9 \pmod{23} & 7^2 \equiv 3 \pmod{23} & 11^2 \equiv 6 \pmod{23} \\ 4^2 \equiv 16 \pmod{23} & 8^2 \equiv 18 \pmod{23} & \end{array}$$

The quadratic residues of $p = 23$ are $\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$

The number of quadratic residues for a given p is $\frac{p-1}{2}$. This was mentioned in class. First of all, there can't be more than $\frac{p-1}{2}$, since $x^2 \equiv (-x)^2 \pmod{p}$. There also can't be less than $\frac{p-1}{2}$, since all the squares of numbers between 1 and $\frac{p-1}{2}$ are all distinct. Wouldn't this make a lovely test question to explain why! (hint, hint, nudge, nudge)

4. Given that the prime p satisfies $3p = a^2 + 5b^2$ for some integers a and b , find explicit integers A and B (in terms of a and b) such that $2p = A^2 + 5B^2$.

Hint: The product of $a + b\sqrt{-5}$ times its complex conjugate equals $3p$. What would such a product become if one were to replace $a + b\sqrt{-5}$ by $(a + b\sqrt{-5}) \cdot \left(\frac{1+E\sqrt{-5}}{3}\right)$ where E is 1 or -1? You'll have to justify why the numbers you find are actually integers.

Suppose $3p = a^2 + 5b^2$. Consider the number $(a + b\sqrt{-5})\left(\frac{1+E\sqrt{-5}}{3}\right)$. Expanding and collecting terms, we have

$$(a + b\sqrt{-5})\left(\frac{1 + E\sqrt{-5}}{3}\right) = \frac{a - 5Eb}{3} + \frac{Ea + b}{3}\sqrt{-5} = A + B\sqrt{-5}$$

if we define $A = \frac{a-5Eb}{3}$ and $B = \frac{Ea+b}{3}$. Multiplying by the conjugates on each sides results in

$$\begin{aligned} A^2 + 5B^2 &= (A + B\sqrt{-5})(A - B\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5})\left(\frac{1 + E\sqrt{-5}}{3}\right)\left(\frac{1 - E\sqrt{-5}}{3}\right) \\ &= (a^2 + 5b^2)\left(\left(\frac{1}{3}\right)^2 + 5\left(\frac{E^2}{3}\right)^2\right) = 3p \cdot \frac{2}{3} = 2p \end{aligned}$$

We must now show that by choosing the right E , then A and B are integers.

Consider the equation $3p = a^2 + 5b^2$ modulo 3. Then

$$0 \equiv a^2 + 5b^2 \equiv a^2 - b^2 \equiv (a + b)(a - b) \pmod{3}$$

Since 3 is a prime, this says that either $a + b \equiv 0 \pmod{3}$ or $a - b \equiv 0 \pmod{3}$.

Suppose $a + b \equiv 0 \pmod{3}$. Then $a + b = 3k$ for some integer k . If we let $E = 1$, then A and B are both integers:

$$\begin{aligned} A &= \frac{a - 5b}{3} = \frac{(a + b) - 6b}{3} = \frac{3k - 6b}{3} = k - 2b \\ B &= \frac{a + b}{3} = \frac{3k}{3} = k \end{aligned}$$

Now suppose $a - b \equiv 0 \pmod{3}$. Then $a - b = 3l$ for some integer l . If we let $E = -1$, then A and B are both integers:

$$\begin{aligned} A &= \frac{a + 5b}{3} = \frac{(a - b) + 6b}{3} = \frac{3l + 6b}{3} = l + 2b \\ B &= \frac{-a + b}{3} = \frac{-(a - b)}{3} = \frac{-3l}{3} = -l \end{aligned}$$

This proves that in either case, a single value of E makes both A and B integers.

5. (a) If $p = a^2 + 5b^2$, prove that $p \equiv 1$ or $9 \pmod{20}$.
 (b) If $2p = a^2 + 5b^2$, prove that $p \equiv 3$ or $7 \pmod{20}$.

Note: The problem as stated is not correct. This problem is a continuation from the discussion in class, which included the hypothesis that a and b were both positive integers. Otherwise, $p = 5$ is an exception for part (a) since $5 = 0^2 + 5 \cdot 1^2$, and $p = 2$ is an exception for part (b) since $2 \cdot 2 = 2^2 + 5 \cdot 0^2$. We continue the problem assuming that p is odd and $p \neq 5$.

(a) Suppose $p = a^2 + 5b^2$. a and b cannot both be even, otherwise $a^2 + 5b^2$ is even. Likewise, a and b cannot both be odd, otherwise $a^2 + 5b^2$ is even. So one of a or b is even, the other is odd.

Modulo 4, an even square is congruent to 0 and an odd square is congruent to 1. Considering the equation $p = a^2 + 5b^2$ modulo 4, we have $p \equiv a^2 + b^2 \equiv 1 + 0 \equiv 1 \pmod{4}$.

We may also consider the equation modulo 5. Then $p \equiv a^2 \pmod{5}$. The only nonzero squares modulo 5 are 1 and 4. (One show really make sure that $a \not\equiv 0 \pmod{5}$. But this would make $p \equiv 0 \pmod{5}$, which would say $p = 5$ since p is a prime.) Hence $p \equiv 1$ or $4 \pmod{5}$.

Putting these two moduli together, we have either $p \equiv 1 \pmod{4}$, $p \equiv 1 \pmod{5}$ or $p \equiv 1 \pmod{4}$, $p \equiv 4 \pmod{5}$.

Consider $p \equiv 1 \pmod{4}$, $p \equiv 1 \pmod{5}$. From the first equation, we have $p = 1 + 4k$ for some integer k . Then $p = 1 + 4k \equiv 1 \pmod{5}$. Solving for k , we have $4k \equiv 0 \pmod{5}$. The inverse of 4 modulo 5 is 4 (since $4 \cdot 4 \equiv 1 \pmod{5}$). Multiplying by 4 on both sides shows that $k \equiv 0 \pmod{5}$. Hence, there exists an integer l such that $k = 5l$. Plugging this in to the original equation for p results in

$$p = 1 + 4k = 1 + 4(5l) = 1 + 20l \implies p \equiv 1 \pmod{20}$$

We do the same when $p \equiv 1 \pmod{4}$, $p \equiv 4 \pmod{5}$. This time, we have $p = 1 + 4k \equiv 4 \pmod{5}$, or $4k \equiv 3 \pmod{5}$. Multiplying by 4 on both sides gives $k \equiv 2 \pmod{5}$, or $k = 2 + 5l$ for some integer l . Plugging back in,

$$p = 1 + 4k = 1 + 4(2 + 5l) = 9 + 20l \implies p \equiv 9 \pmod{20}$$

We conclude that $p \equiv 1$ or $9 \pmod{20}$.

(b) Suppose $2p = a^2 + 5b^2$. If a and b are both even, then $a^2 + 5b^2$ is divisible by 4, while $2p$ is not, contradiction. If one of a and b is even, the other odd, then $a^2 + 5b^2$ is odd, while $2p$ is even, contradiction. Hence, we must have both a and b odd.

We use a basic fact which is easy to prove: if a is odd, then $a^2 \equiv 1 \pmod{8}$. Consider the equation $2p = a^2 + 5b^2$ modulo 8. Since a and b must both be odd, $2p \equiv 1 + 5 \cdot 1 \equiv 6 \pmod{8}$. Dividing through by 2 results in $p \equiv 3 \pmod{4}$.

Looking at $2p = a^2 + 5b^2$ modulo 5, we have $2p \equiv a^2 \pmod{5}$. As before, $a^2 \equiv 1$ or $4 \pmod{5}$, so $p \equiv 3$ or $2 \pmod{5}$.

Putting the two modulo requirements together, we have $p \equiv 3 \pmod{4}$ and $p \equiv 3 \pmod{5}$ implies $p \equiv 3 \pmod{20}$. Likewise, $p \equiv 3 \pmod{4}$ and $p \equiv 2 \pmod{5}$ implies $p \equiv 7 \pmod{20}$. One can solve these equation by the same techniques as in part (a). We conclude that $p \equiv 3$ or $7 \pmod{20}$.