

1. (a) If $p = 2$, we note that $3 \equiv 1 \pmod{2}$, so 3 is a quadratic residue mod 2 since 1 is a square. If $p = 3$, then $3 \equiv 0 \pmod{3}$ since 0 is a square.

Hence, it remains to prove the claim if p is an odd prime where $p \geq 5$. Let us assume 3 is a quadratic residue mod p . Hence, $(\frac{3}{p}) = 1$. We consider 2 cases on the bases of Theorem 11.4 (c).

Case 1: If $p \equiv -1 \pmod{4}$. Then, $(\frac{3}{p}) = -(\frac{p}{3}) = 1$. Thus, $(\frac{p}{3}) = -1$. This implies that $p^{(3-1)/2} = p \equiv -1 \pmod{3}$. Since 3 and 4 are co-prime, we get that $p \equiv -1 \pmod{12}$.

Case 2: If $p \not\equiv -1 \pmod{4}$. Then, $(\frac{3}{p}) = (\frac{p}{3}) = 1$. This implies that $p^{(3-1)/2} = p \equiv 1 \pmod{3}$. Since p is an odd prime, we note that $3 \not\equiv 2 \pmod{4}$ or $3 \not\equiv 0 \pmod{4}$. This leaves that $3 \equiv 1 \pmod{4}$. Since 3 and 4 are co-prime, we get that $p \equiv 1 \pmod{12}$.

Considering all the cases, we get that $(\frac{3}{p}) = 1$ if $p = 2, 3$ or $p \equiv \pm 1 \pmod{12}$. Proving the converse is trivial as reversing the proof will show that if $p = 2, 3$ or $p \equiv \pm 1 \pmod{12}$, p would be a quadratic residue mod 3. \square

- (b) For $p = 2$, we note that $-3 \equiv -1 \equiv 1 \pmod{2}$, so it is a quadratic residue. Meanwhile for $p = 3$, $-3 \equiv 0 \pmod{3}$, so it is also a quadratic residue. Hence, we concern ourselves with the case where $p \geq 5$. This implies that $(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = 1$. In other words, either both $(\frac{-1}{p})$ and $(\frac{3}{p})$ must be equal. Hence:

$$(\frac{-1}{p}) = (\frac{3}{p})$$

Applying Theorem 11.4 (a), we get that:

$$(-1)^{(p-1)/2} = (\frac{3}{p})$$

We now consider Theorem 11.4 (c), and note that

$$(\frac{3}{p}) \cdot (\frac{p}{3}) = (-1)^{(p-1)/2 \cdot (3-1)/2} = (-1)^{(p-1)/2}$$

We know that $(\frac{3}{p}) \neq 0$ because p is prime and $p \neq 3$, so:

$$(\frac{3}{p}) = (\frac{p}{3}) \cdot (-1)^{(p-1)/2}$$

Substituting the value with the earlier equation gives:

$$\begin{aligned} (-1)^{(p-1)/2} &= (\frac{p}{3}) \cdot (-1)^{(p-1)/2} \\ 1 &= (\frac{p}{3}) \end{aligned}$$

This implies that p is a square mod 3. In \mathbb{F}_3 , only 0 and 1 are squares. We can rule out $p = 0$ because $p \neq 3$. Hence, -3 is a quadratic residue mod p if $p = 2, 3$ or $p \equiv 1 \pmod{3}$. Proving the converse is again trivial as reversing the proof should suffice to show that if $p = 2, 3$ or $p \equiv 1 \pmod{3}$, -3 is a quadratic residue mod p . \square

- (c) By contradiction, we assume that $p \neq 2$ and $p \not\equiv 1 \pmod{4}$. This implies that p is an odd prime where $2 \nmid (p-1)/2$. We note that $x^2 \equiv -y^2 \pmod{p}$. This implies that $-y^2$ is a quadratic residue mod p , so either $\left(\frac{-y^2}{p}\right) = 0$ or 1 . If $\left(\frac{-y^2}{p}\right) = 1 = \left(\frac{-1}{p}\right)\left(\frac{y}{p}\right)\left(\frac{y}{p}\right)$, we note that $\left(\frac{-1}{p}\right) = -1$ since $(p-1)/2$ is odd. This implies that $\left(\frac{y}{p}\right)^2 = -1$. This equation does not have a real solution, a contradiction. Meanwhile, if $\left(\frac{-y^2}{p}\right) = 0$, then with $\left(\frac{-1}{p}\right) = -1$, $\left(\frac{y}{p}\right) = 0$. This implies $p \mid y$, but if $y \neq 0$, then $x^2 + y^2 \geq y^2 > p$, a contradiction, and if $y = 0$, then $p = x^2$, contradicting p being prime. In all cases, we reach a contradiction thus $p = 2$ or $p \equiv 1 \pmod{4}$. \square

- (d) By contradiction, we assume that $p \neq 3$ and $p \not\equiv 1 \pmod{3}$. This leaves that $p \equiv -1 \pmod{3}$. Now we consider that:

$$\begin{aligned} x^2 - xy + y^2 &= p \\ 4x^2 - 4xy + 4y^2 &= 4p \\ (2x - y)^2 + 3y^2 &= 4p \end{aligned}$$

We now consider that:

$$(2x - y)^2 + 3y^2 \equiv 4p \pmod{3}$$

In \mathbb{F}_3 , $1 = 4$ and $3 = 0$. Hence:

$$(2x - y)^2 \equiv p \pmod{3}$$

However, this implies that $(2x - y)^2 \equiv -1 \pmod{3}$. This is a contradiction because -1 is not a square in \mathbb{F}_3 because $\left(\frac{-1}{3}\right) = (-1)^{(3-1)/2} = -1$. \square

2. (a) By contradiction, assume n is even then $n = 2k$ for some integer k . We then note that $2^n - 1 = 4^k - 1$. Note that $4 \equiv 1 \pmod{3}$, so $4^k \equiv 1 \pmod{3}$. Thus, $3 \mid 4^k - 1$ thus $3 \mid 2^n - 1$. However, we note that $3 \nmid 2^n - 1$, contradiction. \square
- (b) We note that $3^n \equiv 1 \pmod{p}$. This implies that 3^n is a quadratic residue mod p , so $\left(\frac{3^n}{p}\right) = 1$. We then note that we can split $\left(\frac{3^n}{p}\right)$ into n products of $\left(\frac{3}{p}\right)$. However, n is odd, so $\left(\frac{3}{p}\right) \neq 0, -1$. This leaves that $\left(\frac{3}{p}\right) = 1$. By 1(a), this implies that $p = 2, 3$ or $p \equiv \pm 1 \pmod{12}$. However, $p \neq 2$ because 2 is even. Meanwhile, $p \neq 3$ because $3 \nmid 3^n - 1$. This leaves that $p \equiv \pm 1 \pmod{12}$ as desired. \square
- (c) For $n = 1$, we note that $1 \mid 2$, so it works. We now assume that $n > 1$. Since from (a), we get that n is odd, so we can express $n = 2k + 1$ for some integer k . Hence, $2^n - 1 = 2 \cdot 4^k - 1$. We then note that $4^2 \equiv 4 \pmod{12}$. This implies that for $k \geq 1$, we get that $4^k \equiv 4 \pmod{12}$ and that $2 \cdot 4^k - 1 \equiv 2 \cdot 4 - 1 \equiv 7 \pmod{12}$. However, we note that since $n > 1$ and is odd, $2^n - 1 \geq 7$ and is also odd. This implies that $2^n - 1$ can be prime factorized into entirely of odd primes of $p_1 p_2 \cdots p_j$. Note that any odd prime p_i has $p_i \mid 2^n - 1$, so it is also $p_i \mid 3^n - 1$. From (b), this implies that $p_i \equiv \pm 1 \pmod{12}$. This is a contradiction because $p_1 p_2 \cdots p_j \equiv \pm 1 \pmod{12}$ and that $7 \not\equiv \pm 1 \pmod{12}$. Thus, it must be that $n = 1$. \square

3. (a) We first note that if $p \equiv 1 \pmod{3}$, from 1(b), we note that $-3 \equiv a^2 \pmod{p}$ for some integer a . We then note that if a is even, we note that $p - a$ is odd and that $p - a \equiv a \pmod{p}$. Hence this conversion allows us to assume there must exist an odd a . Since a is odd, it is in the form $a = 2k + 1$ for some integer k . This gives:

$$\begin{aligned} (2k+1)^2 &\equiv -3 \pmod{p} \\ 4k^2 + 4k + 1 + 3 &\equiv 0 \pmod{p} \\ 4(k^2 + k + 1) &\equiv 0 \pmod{p} \end{aligned}$$

Since $p \equiv 1 \pmod{3}$, we may assume $p \neq 2$ thus an odd prime. Hence, $p \nmid 4$ and so $4 \neq 0 \in \mathbb{F}_p$. From the above expression, we get that $4(k^2 + k + 1) = 0$ in \mathbb{F}_p . Since \mathbb{F}_p is an integral domain, it must be that $k^2 + k + 1 = 0$ in \mathbb{F}_p . We note that the formal derivative of this polynomial is $2x + 1$. We aim to prove that $2k + 1 \neq 0$ in \mathbb{F}_p . By contradiction, $2k + 1 = 0$ in \mathbb{F}_p . We get that $k = -2^{-1} \pmod{p}$ (Note that $p \neq 2$, so 2^{-1} exists). Hence:

$$\begin{aligned} 4k^2 + 4k + 4 &= 0 \\ 4(-2^{-1})^2 + 4(-2^{-1}) + 4 &= 0 \\ 1 - 2 + 4 &= 0 \\ 3 &= 0 \end{aligned}$$

Since $p \equiv 1 \pmod{3}$, we note that $p \neq 3$. This is a contradiction, so it must be that $2k + 1 \neq 0$ in \mathbb{F}_p . We satisfied the conditions for Corollary 11.16, so there exists a $a \in \mathbb{Z}_p$ where $a^2 + a + 1 = 0$ in \mathbb{Z}_p . In other words, by taking the k -th coordinate of a as a_k , we note that $a_k^2 + a_k + 1 = 0$ in $\mathbb{Z}/p^k\mathbb{Z}$. Hence, there is a solution for $x^2 + x + 1 \equiv 0 \pmod{p^k}$. \square

- (b) Let us assume p is a prime where $p \equiv 2 \pmod{3}$.

Claim: If a is an integer where $p \nmid a$, then there exist an integer solution for $x^2 \equiv a \pmod{p}$.

We first note that $p = 3k + 2$ for some integer k . By Fermat's Little Theorem, we note that $a^{p-1} \equiv 1 \pmod{p}$ and $a^p \equiv a \pmod{p}$. Multiplying the two gives that $a^{2p-1} \equiv a \pmod{p}$. We then substitute p to get that $a^{6k+3} \equiv (a^{(2k+1)})^3 \equiv a \pmod{p}$. We note that $a^{(2k+1)}$ is the solution, so we conclude the proof. \square

We now note that $19 \equiv 1 \pmod{3}$, so since 19 is a prime, we get that $p \nmid 19$. Hence, by the claim, there is an integer solution x to $x^3 \equiv 19 \pmod{p}$. In other words, there is a solution to $x^3 - 19 \equiv 0 \pmod{p}$, or that $x^3 - 19 = 0$ in \mathbb{F}_p . The formal derivative for $x^3 - 19$ is $3x^2$. We aim to prove that $3x^2 \neq 0$ in \mathbb{F}_p . By contradiction, $3x^2 = 0$ in \mathbb{F}_p . We first note that \mathbb{F}_p is an integral domain and that $3 \neq p$ thus $3 \neq 0$ in \mathbb{F}_p , so $x^2 = 0$ and consequently, $x = 0$ in \mathbb{F}_p . However, this implies that $x^3 \equiv 0^3 \equiv 19 \pmod{p}$, a contradiction as $p \nmid 19$. Thus, it must be that $3x^2 \neq 0$ in \mathbb{F}_p .

By Corollary 11.16, there exists a $a \in \mathbb{Z}_p$ where $a^3 - 19 = 0$ in \mathbb{Z}_p . In other words, by taking the k -th coordinate of a as a_k , we note that $a_k^3 - 19 = 0$ in $\mathbb{Z}/p^k\mathbb{Z}$. Hence, there is a solution for $x^3 - 19 \equiv 0 \pmod{p^k}$. \square

- (c) Let us use $7 \in \mathbb{Z}_p$ and denote $f(x) = x^3 - 19$. We note that $f(7) = 7^3 - 19 = 324$ and that $f'(7) = 3 \cdot (7)^2 = 147$ in \mathbb{Z}_p . Note that using the definition from HW6 6 (c):

$$324 = 0 + 0 + 0 + 0 + 1 \cdot 3^4 + 1 \cdot 3^5 + 0 + \dots$$

$$147 = 0 + 1 \cdot 3^1 + 1 \cdot 3^2 + 2 \cdot 3^3 + 1 \cdot 3^4 + 0 + \dots$$

This implies that $\nu_3(324) = 4$ and $\nu_3(147) = 1$. In other words, $\nu_3(f(7)) > 2\nu_3(f'(7))$. We can apply Hensel's Lemma and get that there exist a $\alpha \in \mathbb{Z}_p$ where $f(\alpha) = 0$. Take the k -th coordinate of α as a_k and we see that $a_k^3 - 19 = 0$ in $\mathbb{Z}/3^k\mathbb{Z}$. This translates to that there exist an integer solution to $x^3 - 19 \equiv 0 \pmod{3^k}$. \square

4. (a) We denote $f(x) = x^{46} + 69x + 23$. We first note that both $23 \mid 69$ and $23 \mid 23$. Thus, we note that in $\mathbb{F}_{23}[x]$, $x^{46} + 69x + 23 = x^{46}$. By contradiction, let us assume that the polynomial is reducible and that $f(x) = g(x)h(x)$ in $\mathbb{Z}[x]$. This implies that $g(x)h(x) = x^{46}$ in $\mathbb{F}_{23}[x]$.

Claim: At least $g(x)$ or $h(x)$ is equal to perfect powers, meaning polynomials in the form x^k in $\mathbb{F}_{23}[x]$.

By contradiction, they are both equal to the form $h(x) = x^m a_{m-1} x^{m-1} + \cdots + a_r x^r$ and $g(x) = x^n + b_{n-1} x^{n-1} + \cdots + b_s x^s$ where all a_r and b_r are non-zeros in \mathbb{F}_{23} . We then get $g(x)h(x) = x^{mn} + \cdots + b_s a_r x^{r+s}$. Since \mathbb{F}_{23} is an integral domain, we get that $b_s a_r x^{r+s}$ is a non-zero term, which implies $f(x)$ cannot be equal to a perfect power, a contradiction. If only one of them is equal to a perfect power, where we assume $h(x) = x^m a_{m-1} x^{m-1} + \cdots + a_r x^r$ and $g(x) = x^n$ where a_r is non-zero in \mathbb{F}_{23} . This means $h(x)g(x) = x^{mn} + \cdots + a_r x^{r+n}$ and the same contradiction follows with the non-zero term $a_r x^{r+n}$. Hence, both $g(x)$ and $h(x)$ are equivalent to perfect powers in $\mathbb{F}_{23}[x]$. \square

Since $g(x) = x^m$ and $h(x) = x^n$ in \mathbb{F}_{23} , we note that $g(0) = 0$ and $h(0) = 0$ in \mathbb{F}_{23} . This implies that in \mathbb{Z} , $23 \mid g(0)$ and $23 \mid h(0)$, which implies $23^2 \mid f(0)$. However, we note that $f(0) = 23$ and $23^2 \nmid 23$, a contradiction. Thus, it must be that $f(x)$ is irreducible in $\mathbb{Z}[x]$. \square

- (b) We consider $f(x) = x^{46} + 69x + 2025$. Hence, we note that $f(0) = 2025$ and $f'(0) = 46 \cdot 0^{45} + 69 = 69$ in \mathbb{Z}_3 . Note that using the definition from HW6 6 (c):

$$2025 = 0 + 0 + 0 + 0 + 1 \cdot 3^4 + 2 \cdot 3^5 + 2 \cdot 3^6 + 0 + \cdots$$

$$69 = 0 + 2 \cdot 3^1 + 1 \cdot 3^2 + 2 \cdot 3^3 + 0 + \cdots$$

This implies that $\nu_3(2025) = 4$ and $\nu_3(69) = 1$. In other words, $\nu_3(f(0)) > 2\nu_3(f'(0))$. We apply Hensel's Lemma and get that there exist a $\alpha \in \mathbb{Z}_3$ where $f(\alpha) = 0$. In other words, we found such root. \square