See Below!

(a) (i) State, without proof, the Law of Quadratic Reciprocity for the (2)

Legendre symbol.

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}$$

p and q ~~both odd~~.
distinct odd primes.

$(a,n)=1$

? $x^2 \equiv a \pmod{n}$ soluble?

$$n = \prod_{p^h \| n} p^h$$

check $x^2 \equiv a \pmod{p^h}$ is soluble for all $p^h \| n$.

(ii) Determine the primes p for which 20 is a quadratic residue modulo p. ③

Need $\left(\frac{20}{p}\right) = 1$ $(p \neq 2, 5)$

$$\left(\frac{20}{p}\right) = \left(\frac{2^2 \cdot 5}{p}\right) = \left(\frac{2}{p}\right)^2 \left(\frac{5}{p}\right) = \left(\frac{5}{p}\right)$$

By Quad. Recip. have

$$\left(\frac{5}{p}\right) = (-1)^{\frac{1}{4}(5-1)(p-1)} \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)$$

$$p \equiv \underline{\underline{1}}, 2, 3, \underline{\underline{4}} \pmod 5$$

The squares mod 5 are $1^2, 2^2, 3^2, 4^2 \pmod 5$
$\equiv 1, 4, 4, 1$

So if 20 is a quadratic residue mod p, then p must be $\equiv 1$ or $4 \pmod 5$.

(b) (i) Show that when k is a natural number, then $5k+2$ must be divisible by a prime p satisfying $p \equiv \pm 2 \pmod 5$ ④

Suppose, by way of deriving a contradiction, that $5k+2$ is not divisible by any prime p with $p \equiv \pm 2 \pmod 5$.

Then $5k+2$ is divisible by primes p with

$p \equiv 1 \pmod 5$ or ~~$p \equiv 4 \pmod 5$~~.

$p \equiv -1 \pmod 5$.

Then we have $5k+2 = p_1 p_2 \cdots p_s$, say, where

$p_i \equiv \pm 1 \pmod 5$

$\Rightarrow p_1 p_2 \cdots p_s \equiv \pm 1 \pmod 5$.

But $2 \not\equiv \pm 1 \pmod 5$. /. *,

This contradiction shows that $5k+2$ is divisible by a prime p with $p \equiv \pm 2 \pmod 5$. //

(iii) Show that ⑤

$$20y^2 - 1 = x^3(5x^2+2)$$

has no solutions in integers x and y.

Observe that when $x \neq 0$ then $5x^2+2$ is divisible by a prime $p \equiv \pm 2 \pmod 5$. with p odd.

If $x = 0$, then $20y^2 - 1 = 0$. This is not soluble with $y=0$ ✓ or $|y| \neq 0$ since then $20y^2 > 1$.

If there is a solution (x, y), we take p to be any prime divisor of $5x^2+2$ with $p \equiv \pm 2 \pmod 5$, and we consider

$$20y^2 - 1 \equiv 0 \pmod p.$$

But then $p \equiv \pm 2 \pmod 5$

$$y^2 \equiv (20)^{-1} \pmod p$$

$$\Rightarrow \left(\frac{(20)^{-1}}{p}\right) = 1 \Rightarrow \left(\frac{20}{p}\right) = 1,$$

and this is possible only when $p \equiv \pm 1 \pmod 5$.

So this contradiction shows there are no solns. //

※

(c) (i) State a version of Hensel's Lemma. (7)

Let $f(x) \in \mathbb{Z}[x]$. Suppose that $f(a) \equiv 0 \pmod{p^j}$, and that $p^\tau \| f'(a)$. Then if $j \geq 2\tau+1$, it follows that:

(i) whenever $b \equiv a \pmod{p^{j-\tau}}$, one has $f(b) \equiv f(a) \pmod{p^j}$, and $p^\tau \| f'(b)$;

→ (ii) there exists a unique residue $t \pmod p$ with $f(a + tp^{j-\tau}) \equiv 0 \pmod{p^{j+1}}$.

" $a' \equiv a - \dfrac{p^{-\tau} f(a)}{p^{-\tau} f'(a)} \pmod{p^{j+1}}$ "

(ii) Let n be a natural number. How many solutions does the congruence

$$x^2 - x - 1 \equiv 0 \pmod{5^n}$$

have distinct modulo 5^n? Explain your answer.

Mod 5: Check $0^2 - 0 - 1 \equiv 0 \pmod 5$ ✗

$1^2 - 1 - 1 \equiv 0 \pmod 5$ ✗

$2^2 - 2 - 1 \equiv 0 \pmod 5$ ✗

$\rightsquigarrow 3^2 - 3 - 1 \equiv 0 \pmod 5$ ✓

$4^2 - 4 - 1 \equiv 0 \pmod 5$ ✗

$f(x) := x^2 - x - 1 \Rightarrow f'(x) = 2x - 1$

So $5^1 \| f'(3) = 2 \cdot 3 - 1$. So $\tau = 1$.

Observe that if $x^2 - x - 1 \equiv 0 \pmod{5^n}$, then

then $4x^2 - 4x - 4 \equiv 0 \pmod{5^n}$

$$\Rightarrow (2x-1)^2 - 5 \equiv 0 \pmod{5^n}$$

Then $5 \mid (2x-1)$, and hence $5^2 \mid (2x-1)^2$,

and hence $-5 \equiv 0 \pmod{5^n}$ when $n \geq 2$. #

So there are no solutions when $n \geq 2$.

There is one solution when $n = 1$.

(iii) How many solutions does the congruence

$$x^2 - x - 1 \equiv 0 \pmod{19^n}$$

have distinct modulo 19^n? Explain your answer.

If $x^2 - x - 1 \equiv 0 \pmod{19^n}$, then

$4x^2 - 4x - 4 \equiv 0 \pmod{19^n}$,

so $(2x-1)^2 - 5 \equiv 0 \pmod{19^n}$.

"disc $= b^2 - 4ac$"
$ax^2 + bx + c$
$(-1)^2 - 4 \cdot 1 \cdot (-1)$
$= 5$.

So $\left(\frac{5}{19}\right) = +1$ ($\Rightarrow \exists\, a \in \mathbb{Z}$ with $(a, 19) = 1$, s.t. $a^2 \equiv 5 \pmod{19}$

$\Rightarrow 2x - 1 \equiv \pm a \pmod{19}$

gives a solution $\pmod{19}$)

But $\left(\frac{5}{19}\right) = (-1)^{\frac{1}{4}(5-1)(19-1)} = 1$

$\left(\frac{19}{5}\right) = \left(\frac{-1}{5}\right) = (-1)^{\frac{1}{2}(5-1)} = 1$.

So there are two solutions mod 19. Have if

$$f(x) = x^2 - x - 1,$$

then $f'(x) = 2x - 1$.

But if x is a solution mod 19, then

$$((2x-1)^2, 19) = (5, 19) = 1 \Rightarrow 19 \nmid 2x-1.$$

So Hensel applies with $\tau = 0$, and so the two solutions modulo 19 lift uniquely to 2 solutions modulo 19^n, for each n.

So there are precisely 2 solutions modulo 19^n for each n. //

Show that the number of solutions of the congruence

$$x^{10} \equiv 1 \pmod{55^2}$$

is precisely 100.

Observe that $55^2 = 5^2 \cdot 11^2$, and if $N(m)$ is the number of solutions of $x^{10} \equiv 1 \pmod{m}$, then $N(55^2) = N(5^2) \cdot N(11^2)$ by Chinese Remainder Theorem.

solutions of $x^{10} \equiv 1 \pmod{5^2}$

Note that if $(x, 5) = 1$ then $x^{\varphi(5^2)} \equiv 1 \pmod{5^2}$ by Euler's Theorem, so $x^{20} \equiv 1 \pmod{5^2}$.

$$\Downarrow$$

$$x^{10} \equiv \pm 1 \pmod{5^2}$$

Also if $(x, 11) = 1$ we have

$$x^{10} \equiv 1 \pmod{11}$$ by Fermat's Little Theorem.

So $x^{10} \equiv 1 \pmod{11}$ has 10 solutions

By Hensel each lifts uniquely to a solution mod 11^2.

OR observe that there are primitive roots $g_1 \bmod 5^2$ and $g_2 \bmod 11^2$.

If $x^{10} \equiv 1 \pmod{5^2}$ then $x \equiv g_1^r \pmod{5^2}$, for some integer r with $1 \le r \le 20$. Then we have

$$(g_1^r)^{10} \equiv 1 \pmod{5^2}.$$

So $10r$ must be divisible by $\varphi(5^2) = 20$.

$\Rightarrow 2 \mid r$. Hence there are $\frac{20}{2} = 10$ solutions mod 5^2.

So $N(5^2) = 10$.

Similarly have $x^{10} \equiv 1 \pmod{11^2}$

$\Rightarrow x \equiv g_2^s \pmod{11^2}$ with $1 \le s \le 110$.

and then

$$(g_2^s)^{10} \equiv 1 \pmod{11^2}$$

$\Rightarrow$ $10s$ is divisible by $\varphi(11^2) = 110$.

$\Rightarrow$ s is divisible by 11,

so there are 10 solns. $\pmod{11^2}$.

Then $N(5^2) = 10$ & $N(11^2) = 10$

$\Rightarrow N(55^2) = 10 \cdot 10 = 100.$

Show that the number of solutions of the congruence

$$X^{2p} \equiv 1 \pmod{p^2}$$

is precisely $2p$.

(H)

(a) Let p be a prime, and define $f(x) = x - x^p$. Apply Hensel's Lemma to show ~~that~~ whenever b ~~satisfies~~

$$f(b) \equiv 0 \pmod{p^n},$$

then $$f(b^p) \equiv 0 \pmod{p^{n+1}}.$$

(b)

For which integers c are there solutions of

$$x^{p^n} - x^{p^{n-1}} + c \equiv 0 \pmod{p^n}?$$

Explain your answer.