

18.781: Selected solutions of problems from PS 6 and 7

The answers are in reverse order from the order in the book.

3.3 (20) This was done in class. Consider the equation

$$(1) \quad X^2 - Y^2 \equiv a \pmod{p}.$$

The number of solutions to this equation is given by the sum

$$\sum_Y \left(1 + \left(\frac{Y^2 + a}{p}\right)\right),$$

where Y runs over a complete residue system. Pulling out the 1, we see that this sum is equal to

$$p + \sum_{Y=1}^p \left(\frac{Y^2 + a}{p}\right).$$

and hence to finish the exercise it is enough to show that (1) has $p - 1$ solutions. For this, consider the change of variable $X = U + V$ and $Y = U - V$. This change of variable transforms the equation (1) into the equation

$$4UV \equiv a \pmod{p}.$$

This equation has $p - 1$ solutions. For if we fix a non-zero value u for U , there is a unique value v for V such that the equation holds, since $(4a, p) = 1$ by assumption.

So the only thing left to check is that the map

$$f : (\text{pairs of congruence classes } (U, V) \pmod{p}) \rightarrow (\text{pairs of congruence classes } (X, Y) \pmod{p})$$

which sends (U, V) to $(U + V, U - V)$ is a bijection. For this, consider the map

$$g : (\text{pairs of congruence classes } (X, Y) \pmod{p}) \rightarrow (\text{pairs of congruence classes } (U, V) \pmod{p})$$

which sends (X, Y) to $(X + Y, X - Y)$. Then $g \circ f$ sends (U, V) to $(2U, 2V)$ and $f \circ g$ sends (X, Y) to $(2X, 2Y)$. Since $(2, p) = 1$ it follows that $g \circ f$ and $f \circ g$ are bijections, which implies that g and f are also bijections.

3.3 (14) By quadratic reciprocity and the fact that $p \equiv 1 \pmod{4}$ we have

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

3.3 (7) If $x^2 + y^2 \equiv 0 \pmod{p}$, then let \bar{x} be an integer so that $x\bar{x} \equiv 1 \pmod{p}$. Then we have $-1 \equiv (y\bar{x})^2 \pmod{p}$ which implies that -1 is a square so $p \equiv 1 \pmod{4}$. Conversely, if $p \equiv 1 \pmod{4}$, then we showed in theorem 2.15 that p can be written as a sum of two squares. Thus the answer is if and only if $p \equiv 1 \pmod{4}$ or $p = 2$ ($2 = 1^2 + 1^2$).

3.2 (22) Letting Y run over a complete residue system, we find that the number of solutions is equal to

$$\sum_Y \left(1 + \left(\frac{\bar{a} - \bar{a}bY^2}{p}\right)\right) = p + \left(\frac{-\bar{a}}{p}\right) \sum_Y \left(\frac{bY^2 - 1}{p}\right) = p + \left(\frac{-\bar{a}b}{p}\right) \sum_Y \left(\frac{Y^2 - \bar{b}}{p}\right),$$

where we write \bar{a} (resp. \bar{b}) for an integer so that $a\bar{a} \equiv 1 \pmod{p}$ (resp. $b\bar{b} \equiv 1 \pmod{p}$). By exercise 3.3 20, the above is equal to

$$p - \left(\frac{-\bar{a}b}{p} \right).$$

On the other hand,

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

so the above is equal to

$$p - \left(\frac{-ab}{p} \right)$$

as desired.

3.2 (13) To see that there are infinitely many primes p congruent to 1 mod 3, note that this is equivalent to saying that p is a square mod 3. Thus it is enough to show that there are infinitely many primes with $\left(\frac{p}{3}\right) = 1$. Suppose that there were finitely many p_1, \dots, p_n , and consider the number

$$N = (4p_1 \cdots p_n)^2 + 3.$$

Since $N \equiv 3 \pmod{4}$ there exists a prime $p \equiv 3 \pmod{4}$ not equal to one of the p_1, \dots, p_n which divides N . Now compute

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

using quadratic reciprocity. This is a contradiction.

As for the case of $p \equiv -1 \pmod{3}$, suppose by contradiction again that there are finitely many, and let p_1, \dots, p_n be the odd ones and write

$$N = (p_1 \cdots p_n)^2 - 3.$$

Then $N \equiv -2 \pmod{8}$, so $N/2 \equiv 3 \pmod{4}$. This implies that there exists a prime $p \equiv 3 \pmod{4}$ which divides $N/2$ and hence also N . Now we compute again

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

by quadratic reciprocity, so we must have $p \equiv -1 \pmod{3}$. This is a contradiction.

3.2 (8) Note that

$$\left(\frac{10}{p} \right) = \left(\frac{2}{p} \right) \left(\frac{5}{p} \right) = \left(\frac{2}{p} \right) \left(\frac{p}{5} \right)$$

by quadratic reciprocity. We consider two cases.

Case 1: $p \equiv 1, 7 \pmod{8}$ or equivalently $\left(\frac{2}{p}\right) = 1$. In this case, we want $\left(\frac{p}{5}\right) = 1$ which means that $p \equiv 1, 4 \pmod{5}$. Combining the above congruences we get that $p \equiv 1, 9, 31, 39 \pmod{40}$.

Case 2: $p \equiv 3, 5 \pmod{8}$ or equivalently $\left(\frac{2}{p}\right) = -1$. In this we want $\left(\frac{p}{5}\right) = -1$ which means that $p \equiv 2, 3 \pmod{5}$. This gives $p \equiv 3, 13, 27, 37 \pmod{40}$.

Putting it all together we have

$$p \equiv 1, 3, 9, 13, 27, 31, 37, 39 \pmod{40}$$

as our final answer.

3.1 (23) By Hensel's lemma, the number of solutions to the equation $X^2 \equiv a \pmod{p^\alpha}$ is equal to the number of solutions to the equation $X^2 \equiv a \pmod{p}$ since $(2, p) = 1$ and $(a, p) = 1$, for these two conditions imply that if β is any solution then 2β is not divisible by p . Now for $\alpha = 1$ the result is basically the definition of the quadratic residue symbol.

3.1 (18) Let γ be a primitive root modulo p , so that the set

$$\{\gamma, \gamma^2, \dots, \gamma^{p-1}\}$$

is a reduced residue system. Then γ^i is a cubic residue if and only if $i \equiv 3\lambda \pmod{p-1}$ for some λ (if confused about this please ask). Now if $3|p-1$ this means simply that i is divisible by 3, so in this case there are $(p-1)/3$ cubic residues. On the other hand, if $(3, p-1) = 1$, then there exists a number $\bar{3}$ so that $3\bar{3} \equiv 1 \pmod{p-1}$, so in this case every i can be written as

$$i \equiv 3(\bar{3}i) \pmod{p-1},$$

so all elements are cubic residues.

3.1 (15) Consider first the same problem with the interval $[-(p-1)/2, (p-1)/2]$. If j is a quadratic residue in this interval, then $-j$ is also in this interval and

$$\left(\frac{-j}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{j}{p}\right) = 1,$$

since $p \equiv 1 \pmod{4}$. It follows that the sum over the quadratic residues in $[-(p-1)/2, (p-1)/2]$ is zero. Let us call this sum S . Write $S = S_+ \cup S_-$ as the union of its negative elements and positive elements. By the above argument, both S_+ and S_- have $(p-1)/4$ elements. Now write the set of quadratic residues T in $[0, p)$ as a union $T_+ \cup T_-$, where T_+ are those quadratic residues less than or equal to $(p-1)/2$ and T_- are those greater than $(p-1)/2$. Then we have $S_+ = T_+$, and

$$T_- = \{s + p | s \in S_-\}.$$

It follows that

$$\sum_{t \in T} t = \sum_S s + p(p-1)/4 = p(p-1)/4.$$