Primes - Problem Sheet 3 - Solutions

Quadratic residues and quadratic reciprocity

Q1) Use (the supplements to) Quadratic Reciprocity to find congruence conditions on p such that $\left(\frac{-2}{p}\right) = 1$. This gives an alternate proof of the *Reciprocity* step for $p \mid x^2 + 2y^2$. How does this compare with Problem Sheet 2, Question 6?
Solution: We have $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$.

We have need $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1$, or $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = -1$. The first occurs when $p \equiv 1 \pmod 4$ and $p \equiv 1, 7 \pmod 8$. This is if and only if $p \equiv 1 \pmod 8$.

The second occurs when $p \equiv 3 \pmod 4$ and $p \equiv 3, 5 \pmod 8$. This is if and only if $p \equiv 3 \pmod 8$.

Hence $\left(\frac{-2}{p}\right) = 1$ if and only if $p \equiv 1, 3 \pmod 8$.

Comparing this to Sheet 2, Q 6. There we directly showed that $\left(\frac{2}{p}\right) = -1$ and $\left(\frac{-1}{p}\right) = -1$ implies $\left(\frac{-2}{p}\right) = 1$, without knowing that the Legendre symbol is multiplicative: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Q2) Find congruence conditions on p such that $\left(\frac{a}{p}\right) = 1$ for

i) $a = \pm 5$,

ii) $a = \pm 7$,

iii) $a = \pm 6$,

iv) $a = \pm 10$,

v) $a = \pm 21$.

Hence state the corresponding *Reciprocity* steps for these $x^2 + ny^2$, in these cases.

Solution: These are all very similar, so we only deal with $a = \pm 6$, explicitly.

- (Case $a = 6$:) We want $\left(\frac{6}{p}\right) = 1$. But $\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$. So we require $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1$, or $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1$.
  We have $\left(\frac{2}{p}\right) = 1$ iff $p \equiv 1, 7 \pmod 8$ and $\left(\frac{2}{p}\right) = -1$ iff $p \equiv 3, 5 \pmod 8$.
  We have $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(p-1)/2(3-1)/2} = (-1)^{(p-1)/2} = \left(\frac{-1}{p}\right)$, using QR and the first supplement. Therefore $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)\left(\frac{-1}{p}\right)$.
  We want $\left(\frac{p}{3}\right) = \left(\frac{-1}{p}\right) = 1$, or $\left(\frac{p}{3}\right) = \left(\frac{-1}{p}\right) = -1$. But $\left(\frac{p}{3}\right) = 1$ iff $p \equiv 1 \pmod 3$ and $\left(\frac{p}{3}\right) = -1$ iff $p \equiv 2 \pmod 3$. By the first supplement $\left(\frac{-1}{p}\right) = 1$ iff $p \equiv 1 \pmod 4$ and $\left(\frac{-1}{p}\right) = -1$ iff $p \equiv 3 \pmod 4$.
  So we get

$$\begin{aligned}\left(\frac{3}{p}\right) = 1 &\iff p \equiv 1 \pmod 3 \text{ and } p \equiv 1 \pmod 4 \\ &\quad \text{or } p \equiv 2 \pmod 3 \text{ and } p \equiv 3 \pmod 4 \\ &\iff p \equiv 1 \pmod{12} \text{ or } p \equiv 11 \pmod{12}\end{aligned}$$

Similarly

$$\left(\frac{3}{p}\right) = -1 \iff p \equiv 5, 7 \pmod{12}.$$

Put these together with $\left(\frac{2}{p}\right) = \pm 1$. We get

$$\begin{aligned}\left(\frac{6}{p}\right) = 1 &\iff p \equiv 1, 11 \pmod{12} \text{ and } p \equiv 1, 7 \pmod{8} \\ &\quad \text{or } p \equiv 5, 7 \pmod{12} \text{ and } p \equiv 3, 5 \pmod{8} \\ &\iff p \equiv 1, 23 \pmod{24} \text{ or } p \equiv 5, 19 \pmod{24}\end{aligned}$$

So $\left(\frac{6}{p}\right) = 1$ if and only if $p \equiv 1, 5, 19, 23 \pmod{24}$.
[For explanation: we can get these congruences using the Chinese remainder theorem. Or just directly convert to congruence modulo the lcm.
The lcm of 12 and 8 is 24. So the smallest compatible modulus will be 24. We have

$$\begin{aligned}p \equiv 1, 11 \pmod{12} &\iff p \equiv 1, 11, 1+12, 11+12 \pmod{24} \\ &\iff p \equiv 1, 11, 13, 23 \pmod{24}\end{aligned}$$

and

$$\begin{aligned}p \equiv 1, 7 \pmod{8} &\iff p \equiv 1, 7, 1+8, 7+8, 1+16, 7+16 \pmod{24} \\ &\iff p \equiv 1, 7, 9, 15, 17, 23 \pmod{24}.\end{aligned}$$

Requiring both of these to hold means

$$p \equiv 1, 23 \pmod{24}.$$

Similarly for the other congruences.]
Now we use the result that an odd prime $p \nmid n$ has $p \mid x^2 + ny^2 \iff \left(\frac{-n}{p}\right) = 1$. So we obtain the reciprocity step: an odd prime $p \nmid D = -24$ divides $x^2 - 6y^2$ if and only if $p \equiv 1, 5, 19, 23 \pmod{24}$.

- We get $\left(\frac{-6}{p}\right) = 1$, we require $\left(\frac{6}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = 1$ or $\left(\frac{6}{p}\right) = -1$ and $\left(\frac{-1}{p}\right) = -1$.
  For the first, we get

$$p \equiv 1, 5, 19, 23 \pmod{24} \text{ and } p \equiv 1 \pmod{4}$$

so

$$p \equiv 1, 5 \pmod{24}.$$

For the second

$$p \equiv 7, 11, 13, 17 \pmod{24} \text{ and } p \equiv 3 \pmod{4}.$$

(The congruence mod 24 are the 'complementary' ones to the previous list.) So we get

$$p \equiv 7, 11 \mod *24..$$

Overall

$$\left(\frac{-6}{p}\right) = -1 \iff p \equiv 1, 5, 7, 11 \pmod{24}.$$

Use the result that an odd prime $p \nmid n$ has $p \mid x^2 + ny^2$ iff $\left(\frac{-n}{p}\right) = 1$. So we obtain the reciprocity step that an odd prime $p \nmid D = 24$ divides $x^2 + 6y^2$ if and only if $p \equiv 1, 5, 7, 11 \pmod{24}$.

Q3) (Easy cases of Dirichlet's theorem on primes in arithmetic progressions)

i) By directly imitating Euclid's classical proof that there are infinitely many primes, show that there are infinite many primes $p \equiv 3 \pmod 4$. Hint: consider $N_k = 2^2 p_1 p_2 \dots p_k - 1$, where $p_1 = 3, p_2 = 7, \dots$ are the primes of the form $4n + 3$.
Solution: Suppose only finitely many, then consider $N_k = 2^2 p_1 p_2 \dots p_k - 1$, where $p_1, \dots, p_k$ are all such primes $p_i \equiv 3 \pmod 4$.
Then $N_k \equiv 3 \pmod 4$. N_k must be divisible by some prime $p \equiv 3 \pmod 4$. This is because a product of primes $p \equiv 1 \pmod 4$ is necessarily also $1 \pmod 4$.
So some prime $p \equiv 3 \pmod 4$ divides N_k. But our list contains all such primes, and none of them divide N_k since they all leave a remainder of -1. Hence our list is not complete.

ii) By using Lemma 3.8, with $n = 1$, adapt the above proof, to show there are infinitely many primes $p \equiv 1 \pmod 4$.
Solution: This lemma says that an odd prime $p \mid x^2 + y^2$, $\gcd(x, y) = 1$ if and only if $\left(\frac{-4}{p}\right) = 1$. In particular $p \mid x^2 + 1$ implies $\left(\frac{-4}{p}\right) = 1$, which implies $\left(\frac{-1}{p}\right) = 1$, and so $p \equiv 1 \pmod 4$.
Suppose that there are only finitely many primes $\equiv 1 \pmod 4$, say $p_1, \dots, p_k$. Now consider

$$N_k = (2p_1 \cdots p_k)^2 + 1 \,.$$

This must be divisible by some odd prime. But by the above result, any such odd prime divisor is $\equiv 1 \pmod 4$. This must be some prime not on our list, as all primes on our list leave a remainder of 1.
Hence there are infinitely many primes of the form $p \equiv 1 \pmod 4$.

iii) Show that there are infinitely many primes $p \equiv 1 \pmod 3$ and infinitely many primes $p \equiv 2 \pmod 3$.
Solution: For $p \equiv 2 \pmod 3$, take a list $p_1, \dots, p_k$ of all primes $\equiv 2 \pmod 3$. Set

$$N_k = (12p_1 \cdots p_k) - 1 \,.$$

This is odd and $\equiv 2 \pmod 3$, so must be divisible by an odd prime $\equiv 2 \pmod 3$. Otherwise the result is $\equiv 1 \pmod 3$. This prime is not already on the list. Hence the list must be infinite.
For $p \equiv 1 \pmod 3$, we use that an odd prime $p \mid x^2 + 3y^2$ if and only if $\left(\frac{-12}{p}\right) = 1$ if and only if $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 3$.
Take a list $p_1, \dots, p_k$ of all primes $\equiv 1 \pmod 3$. Set

$$N_k = 3(2p_1 \cdots p_k)^2 + 1 \,.$$

This is odd so is divisible by an odd prime. It is $\equiv 1 \pmod 3$, so not divisible by 3. By the above, we have that any prime divisor must be $\equiv 1 \pmod 3$. Dividing by p_k leaves a remainder of 1, so such a prime divisor is not on the list. Hence the list must be infinite.

Q4) (Primes of the form $x^2 - 2y^2$)

i) Show directly that the descent step holds for $x^2 - 2y^2$.
Solution: See problem sheet 2, Q6iia).

ii) Use quadratic reciprocity to determine when $p \mid x^2 - 2y^2$, $\gcd(x, y) = 1$.
Solution: Using a lemma from lectures, we know an odd prime p not dividing $D = 8$ divides $x^2 - 2y^2$ if and only if $\left(\frac{D}{p}\right) = \left(\frac{8}{p}\right) = 1$.
But $\left(\frac{8}{p}\right) = \left(\frac{2}{p}\right)^2\left(\frac{2}{p}\right) = \left(\frac{2}{p}\right)$. And $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv 1, 7 \pmod 8$ using the second supplement to quadratic reciprocity.

iii) Give a condition on when a prime $p = x^2 - 2y^2$.
Solution: We have $p \equiv 1, 7 \pmod 8$ implies $\left(\frac{2}{p}\right) = 1$, which implies $p \mid x^2 - 2y^2$, $\gcd(x, y) = 1$. By the previous part, this means $p = x^2 - 2y^2$, as descent works.
Conversely, if $p = x^2 - 2y^2$, we see that $p \equiv 1, 7 \pmod 8$ by reducing modulo 8.
Hence, for $p \neq 2$, we have $p = x^2 - 2y^2$ if and only if $p \equiv 1, 7 \pmod 8$.

Q5) In this exercise you will evaluate $\left(\frac{2}{p}\right)$ in a different way, using Euler's criterion. Consider $(\mathbb{Z}/p\mathbb{Z})$, and suppose we extend it to $F = (\mathbb{Z}/p\mathbb{Z})[\overline{\zeta_8}]$ which includes (the image of) $\zeta_8 = e^{2\pi i/8}$, a primitive 8-th root of 1. Then any element $x \in F$ can be written

$$x \equiv \sum_{i=0}^{7} a_i \zeta_8^i \pmod p,$$

with addition and multiplication given in the 'natural ways' using the rule $\zeta_8^8 = 1$. (Similar to $\mathbb{C} = \mathbb{R}[i]$, where we write element $x \in \mathbb{R}[i]$ as $x = a + bi$, and use the rule $i^2 = 1$.)

i) Write $\tau = \zeta_8 + \zeta_8^{-1} = \zeta_8 + \zeta_8^7$. Show that $\tau^2 = 2$, hence using Euler's criterion, show

$$\tau^p \equiv \left(\frac{2}{p}\right)\tau \pmod p.$$

Solution: As a complex number, we compute $\tau^2 = (\zeta_8 + \zeta_8^{-1})^2 = \zeta_8^2 + 2 + \zeta_8^{-2}$. But $\zeta_8^2 = \exp(2\pi i/4) = i$, and $\zeta_8^{-2} = -i$. So $\tau^2 = 2$.
By Euler's criterion, we have

$$\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \pmod p.$$

But $2 = \tau^2$, so

$$\left(\frac{2}{p}\right) \equiv \tau^{2(p-1)/2} = \tau^{p-1}.$$

Finally, multiplying by τ gives

$$\left(\frac{2}{p}\right)\tau \equiv \tau^p \pmod p$$

ii) Using the binomial theorem, show that

$$\tau^p \equiv \zeta_8^p + \zeta_8^{-p} \pmod p$$

Solution: We have

$$\tau^p = (\zeta_8 + \zeta_8^{-1})^p = \zeta_8^p + \zeta_8^{-p} + \sum_{i=1}^{p-1} \binom{p}{i} \zeta_8^{p-2i}$$

Since $1 \leq i \leq p-1$, we know $\binom{p}{i} = 0 \pmod{p}$. (There is no way to cancel the prime p using factors in $i!(p-i)!$, since they are all $< p$.)
Hence

$$\tau^p \equiv \zeta_8^p + \zeta_8^{-p} \pmod{p}.$$

iii) For $p \equiv \pm 1, \pm 3 \pmod 8$, evaluate τ^p, and check the result can be written as

$$\tau^p = (-1)^{(p^2-1)/8}\tau \pmod{p}$$

Solution: For $p = 8k+1$, we have

$$\tau^p \equiv \zeta_8 + \zeta_8^{-1} = \tau,$$

and $(-1)^{(p^2-1)/8} = (-1)^{8k^2+2k} = 1$.
Similarly $p = 8k+3$ gives

$$\tau^p \equiv \zeta_8^3 + \zeta_8^{-3} = \zeta_8^4\zeta_8^{-1} + \zeta_8^{-4}\zeta_8^1 = -\zeta_8^{-1} - \zeta_8 = -\tau,$$

and $(-1)^{(p^2-1)/8} = (-1)^{8k^2+2k+1} = -1$.
The other cases are similar.

iv) Conclude that

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Solution: Combining the above, we have

$$\left(\frac{2}{p}\right)\tau \equiv \tau^p \equiv (-1)^{(p^2-1)/8}\tau \pmod 8.$$

Since $\tau^2 \equiv 2 \pmod p$, we can write $\tau^{-1} \equiv 2^{-1}\tau$, where 2^{-1} exists as $\gcd(2,p) = 1$.
So we can cancel τ from both sides to get

$$\left(\frac{2}{p}\right) \equiv (-1)^{(p^2-1)/8} \pmod p.$$

Since both sides are ± 1, this congruence modulo odd prime p is sufficient to get $=$.