Homework 11

Chris Powell

A. Silverman 21.4. Finish the proof of Quadratic Reciprocity (Part II) for the other two cases: primes congruent to 1 modulo 8 and primes congruent to 5 modulo 8.

Proof. Suppose $[p]_8 = [1]_8$. Then $8 \mid p-1$. So for some $k \in \mathbb{Z}$,

$$p - 1 = 8k \quad \Rightarrow \quad \frac{p-1}{2} = 4k.$$

Thus $\#\{2, 4, \ldots, 4k\} = \#\{4k+2, 4k+4 \ldots, 8k\} = 2k$. Now observe that

$$\begin{aligned}
\left[\left(\frac{2}{p}\right)\right]_p &= \left[2^{\frac{p-1}{2}}\right]_p && \text{(Euler's Criterion)} \\
&= [2]_p^{\frac{p-1}{2}} \\
&= [-1]_p^{\frac{p-1}{2}} && \text{("Fundamental formula", page 157.)} \\
&= [-1]_p^{2k} \\
&= \left[(-1)^{2k}\right]_p \\
&= [1]_p .
\end{aligned}$$

Now assume $[p]_8 = [5]_8$. Then $8 \mid p-5$. So for some $k \in \mathbb{Z}$,

$$p - 5 = 8k \quad \Rightarrow \quad p - 1 = 8k + 4 \quad \Rightarrow \quad \frac{p-1}{2} = 4k + 2.$$

Thus $\#\{2, 4, \ldots, 4k+2\} = \#\{4k+4, 4k+4 \ldots, 8k+4\} = 2k+1$. So

$$\begin{aligned}
\left[\left(\frac{2}{p}\right)\right]_p &= \left[2^{\frac{p-1}{2}}\right]_p && \text{(Euler's Criterion)} \\
&= [2]_p^{\frac{p-1}{2}} \\
&= [-1]_p^{\frac{p-1}{2}} && \text{("Fundamental formula", page 157.)} \\
&= [-1]_p^{2k+1} \\
&= \left[(-1)^{2k+1}\right]_p \\
&= [-1]_p .
\end{aligned}$$

Hence, 2 is a QR $\pmod p$ if $p \equiv 1 \pmod 8$, and 2 is a NR if $p \equiv 5 \pmod 8$. ■

B. Silverman 22.7. Let p be a prime satisfying $p \equiv 3 \pmod 4$ and suppose that a is a quadratic residue modulo p.

(a) Show that $x^{(p+1)/4}$ is a solution to the congruence

$$x^2 \equiv \pmod p.$$

Proof. Observe that

$$\begin{aligned}
\left[\left(a^{\frac{p+1}{4}}\right)^2\right]_p &= \left[a^{\frac{p+1}{2}}\right]_p \\
&= \left[a^{\frac{p-1}{2}+1}\right]_p \\
&= \left[a^{\frac{p-1}{2}} \cdot a\right]_p \\
&= \left[a^{\frac{p-1}{2}}\right]_p \cdot [a]_p \\
&= \left[\left(\frac{a}{p}\right)\right]_p \cdot [a]_p && \text{(Euler's Criterion)} \\
&= [1]_p \cdot [a]_p && (a \text{ is a QR } \pmod p) \\
&= [a]_p \,.
\end{aligned}$$

Therefore, $x = a^{\frac{p+1}{4}}$ is a solution to $x^2 \equiv \pmod p$ for all primes $p \equiv 3 \pmod 4$. ■

(b) Find a solution to the congruence $x^2 \equiv 7 \pmod{787}$. (Your answer should be between 1 and 786.)

Since $[787]_4 = [3]_4$, part (a) of this exercise implies that

$$\left[7^{\frac{787+1}{4}}\right]_{787} = \left[7^{144}\right]_{787}$$

is a solution. But by successive squaring (i.e., using the `expmod(7,144,787)` algorithm),

$$\left[7^{144}\right]_{787} = [692]_{787}\,.$$

Thus $x = 692$ is solution to $x^2 \equiv 7 \pmod{787}$ satisying $1 \leqslant x \leqslant 786$.

C. Silverman 22.8. Let p be a prime satisfying $p \equiv 5 \pmod 8$ and suppose that a is a quadratic residue modulo p.

(a) Show that one of the values

$$x = a^{(p+3)/8} \quad \text{or} \quad x = 2a \cdot (4a)^{(p-5)/8}$$

is a solution to the congruence

$$x^2 \equiv a \pmod p.$$

Proof. Observe that

$$\left[\left(a^{\frac{p+3}{8}}\right)^2\right]_p = \left[a^{\frac{p+3}{4}}\right]_p = \left[a^{\frac{p-1}{4}+1}\right]_p = \left[a^{\frac{p-1}{4}} \cdot a\right]_p = [a]_p^{\frac{p-1}{4}} \cdot [a]_p \,.$$

Since a is a QR $\pmod p$, we know $[a]_p = \left[b^2\right]_p$ for some $b \in \mathbb{Z}$, thus

$$\left[\left(a^{\frac{p+3}{8}}\right)^2\right]_p = \left[b^2\right]_p^{\frac{p-1}{4}} \cdot [a]_p = \left[b^{\frac{p-1}{2}}\right]_p \cdot [a]_p = \left[\left(\frac{b}{p}\right)\right]_p \cdot [a]_p \,.$$

If b is a QR $\pmod p$, we're done as then

$$\left[\left(\frac{b}{p}\right)\right]_p \cdot [a]_p = [1]_p \cdot [a]_p = [a]_p \,.$$

So suppose b is not a QR $\pmod p$. Then

$$\left[\left(2a \cdot (4a)^{\frac{p-5}{8}}\right)^2\right]_p = \left[4a^2 \cdot (4a)^{\frac{p-5}{4}}\right]_p = \left[4^{\frac{p-5}{4}+1} \cdot a^{\frac{p-5}{4}+1} \cdot a\right]_p \,.$$

Simplifying further, we get

$$\left[4^{\frac{p-5}{4}+1} \cdot a^{\frac{p-5}{4}+1} \cdot a\right]_p = \left[4^{\frac{p-1}{4}} \cdot a^{\frac{p-1}{4}} \cdot a\right]_p = [4]_p^{\frac{p-1}{4}} \cdot [a]_p^{\frac{p-1}{4}} \cdot [a]_p \,.$$

But 4 and a are QR's $\pmod p$, so we can write that last expression as

$$\left[2^2\right]_p^{\frac{p-1}{4}} \cdot \left[b^2\right]_p^{\frac{p-1}{4}} \cdot [a]_p = \left[2^{\frac{p-1}{2}}\right]_p \cdot \left[b^{\frac{p-1}{2}}\right]_p \cdot [a]_p \,,$$

and by Euler's Criterion,

$$\left[2^{\frac{p-1}{2}}\right]_p \cdot \left[b^{\frac{p-1}{2}}\right]_p \cdot [a]_p = \left[\left(\frac{2}{p}\right)\right]_p \cdot \left[\left(\frac{b}{p}\right)\right]_p \cdot [a]_p$$

Finally, as $[p]_8 = [5]_8$ and b is a QR $\pmod p$, the last expression gives

$$[-1]_p \cdot [-1]_p \cdot [a]_p = [(-1) \cdot (-1) \cdot a]_p = [1 \cdot a]_p = [a]_p \,.$$

■

(b) Find a solution to the congruence $x^2 \equiv 5 \pmod{541}$. (Give an answer lying between 1 and 540.)

First, note that the modulus 541 is a prime satisfying $[541]_8 = [5]_8$, so we can apply the above result. Since

$$\left[5^{\frac{541-1}{4}}\right]_{541} = \left[5^{\frac{540}{4}}\right]_{541} = \left[5^{135}\right]_{541} = [1]_{541}\,,$$

we know $x = 5^{\frac{541+3}{8}}$ is a solution. But

$$\left[5^{\frac{541+3}{8}}\right]_{541} = \left[5^{\frac{544}{8}}\right]_{541} = \left[5^{68}\right]_{541}\,,$$

and by successive squaring, we obtain

$$\left[5^{68}\right]_{541} = [345]_{541}\,.$$

Hence, $x = 345$ is solution to $x^2 \equiv 5 \pmod{541}$ satisfying $1 \leqslant x \leqslant 540$.

(c) Find a solution to the congruence $x^2 \equiv 13 \pmod{653}$. (Give an answer lying between 1 and 652.)

First, note that the modulus 653 is a prime satisfying $[543]_8 = [5]_8$, so we can again apply the above result. As

$$\left[13^{\frac{653-1}{4}}\right]_{643} = \left[13^{\frac{652}{4}}\right]_{653} = \left[13^{163}\right]_{653} = [-1]_{653}\,,$$

we know $x = (2 \cdot 13) \cdot (4 \cdot 13)^{\frac{653-5}{8}}$ is a solution. But

$$\left[(2 \cdot 13) \cdot (4 \cdot 13)^{\frac{653-5}{8}}\right]_{653} = \left[(26) \cdot (54)^{\frac{648}{8}}\right]_{653} = \left[(26) \cdot (54)^{81}\right]_{653}\,,$$

and

$$\begin{aligned}
\left[26 \cdot 52^{81}\right]_{653} &= [26]_{653} \cdot \left[52^{81}\right]_{653} \\
&= [26]_{653} \cdot [212]_{653} \qquad \text{(successive squaring)} \\
&= [26 \cdot 212]_{653} \\
&= [5512]_{653} \\
&= [288]_{653}\,.
\end{aligned}$$

Hence, $x = 288$ is solution to $x^2 \equiv 13 \pmod{653}$ satisfying $1 \leqslant x \leqslant 652$.

k

D. Silverman 22.9. Let p be a prime that is congruent to 5 modulo 8. Write a program to solve the congruence

$$x^2 \equiv a \pmod{p}$$

using the method described in the previous exercise and successive squaring. The output should be a solution satisfying $0 \leqslant x < p$. Be sure to check that a is a quadratic residue, and return an error message if it is not. Use your program to solve the congruences

$$x^2 \equiv 17 \pmod{1021}, \quad x^2 \equiv 23 \pmod{1021}, \quad x^2 \equiv 31 \pmod{1021}.$$

```
def expmod(a, k, m):
    """compute a^k mod m"""
    b = 1
    while k:
        if k % 2 == 1:
            b = (b * a) % m
        a, k = (a ** 2) % m, k // 2
    return b

def residue(n, p):
    """Return each a  b^n mod p for some integer b and modulus p; n
        =2,3"""
    R = []
    for i in range(p):
        R += [(i**n) % p]
    return set(R)


def hw11(a, p):
    """Return solution-pair to x^2=a (mod p) for prime p=5 (mod 8)
        """
    if a not in residue(2, p):
        return str(a)+" is not a quadratic residue modulo "+str(p)+"
            ."
    if expmod(a, ((p - 1) // 4), p) == 1:
        x = expmod(a, ((p + 3) // 8), p)
        return x, -x % p
    else:
        x = ((2 * a) * expmod(4 * a, ((p - 5) // 8), p)) % p
        return x, -x % p
```

Proof. Since the `residue()` and `expmod()` algorithms have already been shown to terminate and return the correct output, it immediately follows that that `hw11()` algorithm must terminate. It remains to show correctness. Let a and p be the respective values of the python variables a and p. Assume p is prime such that $p \equiv 5 \pmod{8}$. Now either a is a quadratic residue modulo p, or it isn't. If a is not, then by correctness of `residue()`, the first `if` statement will evaluate to true and the program will return an error message; otherwise, it will evaluate to false and execution proceeds.

So suppose a is a quadratic residue modulo p. Then by Exercise C, every solution to the congruence $x^2 \equiv 5 \pmod{p}$ is of the form

$$a^{\frac{p+3}{8}} \quad \text{or} \quad 2a \cdot (4a)^{(p-5)/8},$$

depending on whether

$$\left[a^{\frac{p-1}{4}}\right]_p = [1]_p \quad \text{or} \quad \left[a^{\frac{p-1}{4}}\right]_p = [-1]_p .$$

But those are exactly the two remaining termination conditions, and in each case the program returns the appropriate form by correctness of `expmod()`. Hence the program returns correctly. ∎

`hw11(17,1021)` returns `(494,527)`
`hw11(23,1021)` returns `(858,163)`
`hw11(31,1021)` returns `'31 is not a quadratic residue modulo 1021.'`