Homework 12

Chris Powell

A. Silverman 22.1. Use the Law of Quadratic Reciprocity to compute the following Legendre Symbols.

(a) $\left(\frac{85}{101}\right)$

$$\begin{aligned}
\left(\frac{85}{101}\right) &= \left(\frac{5}{101}\right)\left(\frac{17}{101}\right) && (101 \text{ is an odd prime})\\
&= \left(\frac{101}{5}\right)\left(\frac{101}{17}\right) && (101 \equiv 1 \pmod 4)\\
&= \left(\frac{1}{5}\right)\left(\frac{101}{17}\right) && (101 \equiv 1 \pmod 5)\\
&= 1 \cdot \left(\frac{101}{17}\right) && (1 \text{ is a QR } \pmod 5)\\
&= \left(\frac{16}{17}\right) && (101 \equiv 16 \pmod{17})\\
&= \left(\frac{2^4}{17}\right)\\
&= \left(\left(\frac{2}{17}\right)\right)^4 && (101 \text{ on odd prime})\\
&= 1^4 && (101 \text{ on odd prime})\\
&= 1.
\end{aligned}$$

(b) $\left(\frac{29}{541}\right)$

$$\begin{aligned}
\left(\frac{29}{541}\right) &= \left(\frac{541}{20}\right) && (29, 541 \equiv 1 \pmod 4)\\
&= \left(\frac{19}{29}\right) && (541 \equiv 19 \pmod{29})\\
&= \left(\frac{29}{19}\right) && (29 \equiv 1 \pmod 4)\\
&= \left(\frac{10}{19}\right) && (29 \equiv 10 \pmod{29})\\
&= \left(\frac{2}{19}\right)\left(\frac{5}{19}\right) && (19 \text{ is an odd prime})\\
&= (-1)\left(\frac{5}{19}\right) && (19 \equiv 3 \pmod 8)\\
&= (-1)\left(\frac{19}{5}\right) && (19 \text{ is an odd prime})\\
&= (-1)\left(\frac{4}{5}\right) && (19 \equiv 4 \pmod 5)\\
&= (-1)\left(\frac{2^2}{5}\right)\\
&= (-1)\left(\left(\frac{2}{5}\right)\right)^2 && (5 \text{ is an odd prime})\\
&= (-1)(1)^2 && (5 \equiv 5 \pmod 8)\\
&= (-1)(1)\\
&= -1.
\end{aligned}$$

(c) $\left(\frac{101}{1987}\right)$

$$
\begin{aligned}
\left(\frac{101}{1987}\right) &= \left(\frac{1987}{101}\right) && (1987 \equiv 1 \pmod 4)\\
&= \left(\frac{68}{101}\right) && (1987 \equiv 68 \pmod{101})\\
&= \left(\frac{4}{101}\right)\left(\frac{17}{101}\right) && (101 \text{ is an odd prime})\\
&= \left(\frac{2^2}{101}\right)\left(\frac{17}{101}\right) && \\
&= \left(\left(\frac{2}{101}\right)\right)^2\left(\frac{17}{101}\right) && (101 \text{ is an odd prime})\\
&= (-1)^2\left(\frac{17}{101}\right) && (101 \equiv 5 \pmod 8)\\
&= 1 \cdot \left(\frac{17}{101}\right) && \\
&= \left(\frac{17}{101}\right) && \\
&= \left(\frac{101}{17}\right) && (17, 101 \equiv 1 \pmod 4)\\
&= \left(\frac{16}{17}\right) && (101 \equiv 16 \pmod{17})\\
&= \left(\frac{2^4}{17}\right) && \\
&= \left(\left(\frac{2}{17}\right)\right)^4 && (17 \text{ is an odd prime})\\
&= 1^4 && (17 \equiv 1 \pmod 8)\\
&= 1.
\end{aligned}
$$

(d) $\left(\frac{31706}{43789}\right)$

$$
\begin{aligned}
\left(\frac{31706}{43789}\right) &= \left(\frac{2}{43789}\right)\left(\frac{15853}{43789}\right) && \\
&= (-1)\left(\frac{15853}{43789}\right) && (43789 \equiv 5 \pmod 8) \\
&= (-1)\left(\frac{43789}{15853}\right) && (43789 \equiv 5 \pmod 8) \\
&= (-1)\left(\frac{12083}{15853}\right) && (43789 \equiv 12083 \pmod{15853}) \\
&= (-1)\left(\frac{15853}{12083}\right) && (15853 \equiv 1 \pmod 4) \\
&= (-1)\left(\frac{3770}{12083}\right) && (15853 \equiv 3770 \pmod{12083}) \\
&= (-1)\left(\frac{2}{12083}\right)\left(\frac{1885}{12083}\right) && (12083 \text{ is an odd prime}) \\
&= \left(\frac{1885}{12083}\right) && (12083 \equiv 3 \pmod 8) \\
&= \left(\frac{12083}{1885}\right) && (1885 \equiv 1 \pmod 4) \\
&= \left(\frac{773}{1885}\right) && (12083 \equiv 773 \pmod{1885}) \\
&= \left(\frac{1885}{773}\right) && (1885 \equiv 773 \equiv 4 \pmod 4) \\
&= \left(\frac{339}{773}\right) && (1885 \equiv 339 \pmod{773}) \\
&= \left(\frac{773}{339}\right) && (773 \equiv 1 \pmod 4) \\
&= \left(\frac{95}{339}\right) && (773 \equiv 95 \pmod{339}) \\
&= (-1)\left(\frac{339}{95}\right) && (339 \equiv 95 \equiv 3 \pmod 4) \\
&= (-1)\left(\frac{54}{95}\right) && (339 \equiv 54 \pmod{95}) \\
&= (-1)\left(\frac{2}{95}\right)\left(\frac{27}{95}\right) && (95 \text{ is an odd prime}) \\
&= (-1)\left(\frac{27}{95}\right) && (95 \equiv 7 \pmod 8) \\
&= \left(\frac{95}{27}\right) && (95 \equiv 27 \equiv 3 \pmod 4) \\
&= \left(\frac{14}{27}\right) && (95 \equiv 14 \pmod{27}) \\
&= \left(\frac{2}{27}\right)\left(\frac{7}{27}\right) && (27 \text{ is an odd prime}) \\
&= (-1)\left(\frac{7}{27}\right) && (27 \equiv 3 \pmod 8) \\
&= \left(\frac{27}{7}\right) && (27 \equiv 7 \equiv 3 \pmod 4) \\
&= \left(\frac{6}{7}\right) && (27 \equiv 6 \pmod 7) \\
&= \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) && (7 \text{ is an odd prime}) \\
&= \left(\frac{3}{7}\right) && (7 \equiv 7 \pmod 8) \\
&= (-1)\left(\frac{7}{3}\right) && (7 \equiv 3 \equiv 3 \pmod 4) \\
&= (-1)\left(\frac{1}{3}\right) && (7 \equiv 1 \pmod 3) \\
&= -1 && (1 \text{ is a QR } \pmod 3)\,.
\end{aligned}
$$

B. Silverman 22.3. Show that there are infinitely many primes congruent to 1 modulo 3.

Proof. Suppose there are only finitely many primes congruent to 1 modulo 3, say $p_1, \ldots, p_r$. Let

$$A = \left(2\prod_{i=1}^{r} p_i\right)^2 + 3.$$

Then by the Fundamental Theorem of Arithmetic, A has prime factorization $A = \prod_{i=1}^{s} q_i$, where each q_i is distinct. Because each q_i divides A, but no p_i divides A, we may conclude $q_i \neq p_j$ for all i, j. Thus it remains to show that $[q_i]_3 = [1]_3$ for some i. Now since

$$A = \left(2\prod_{i=1}^{r} p_i\right)^2 + 3 = 4\left(\prod_{i=1}^{r} p_i\right)^2 + 3,$$

we can see that $[A]_4 = [3]_4$, so A is odd. Thus each prime factor q_i is odd and so either $[q_i]_4 = [1]_4$ or $[q_i]_4 = [3]_4$ for all i. It cannot be that $[q_i]_4 = [1]_4$ for all i. WLOG, $[q_k]_4 = [3]_4$. Then $[A]_{q_k} = [0]_{q_k}$. This implies $x = 2\prod_{i=1}^{r} p_i$ is a solution to $\left[x^2\right]_{q_k} = [-3]_{q_k}$. In other words, $\left(\frac{-3}{q_k}\right) = 1$. But

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

Hence, $\left(\frac{q_k}{3}\right) = 1$ which implies $[q_k]_3 = [1]_3$. ∎

C. Silverman 22.10. If $a^{m-1} \not\equiv 1 \pmod{m}$, then Fermat's Little Theorem tells us that m is composite. On the other hand, even if

$$a^{m-1} \equiv 1 \pmod{m}$$

for some (or all) a's satisfying $\gcd(a, m) = 1$, we cannot not conclude that m is prime. This exercise describes a way to use Quadratic Reciprocity to check if a number is probably prime.

(a) Euler's Criterion says that if p is prime then

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

Use successive squaring to compute $11^{864} \pmod{1729}$ and use Quadratic Reciprocity to compute $\left(\frac{11}{1729}\right)$. Do they agree? What can you conclude concerning the possible primality of 1729?

The program `expmod(11,864,1729)` returns `1`, thus the successive squaring method gives

$$11^{864} \equiv 1 \pmod{1729}.$$

Now observe that

$$\begin{aligned} \left(\frac{11}{1729}\right) &= \left(\frac{1729}{11}\right) && (1729 \equiv 1 \pmod{4}) \\ &= \left(\frac{2}{11}\right) && (1729 \equiv 2 \pmod{11}) \\ &= -1 && (11 \equiv 3 \pmod{8}). \end{aligned}$$

So 1729 is not a prime.

(b) Use successive squaring to compute the quantities

$$2^{\frac{1293337-1}{2}} \pmod{1293337} \quad \text{and} \quad 2^{129336} \pmod{1293337}.$$

What can you conlude concerning the possible primality of 1293337?

The program `expmod(2,1293336//2,1293337)` returns `429596`, thus the successive squaring method gives

$$2^{\frac{1293337-1}{2}} \equiv 429596 \pmod{1293337}.$$

Clearly, $429596 \not\equiv \pm 1 \pmod{1293337}$ so, by Euler's Criterion, the modulus 1293337 is not a prime.

D. Silverman 24.4.

(a) Start from $259^2 + 1^2 = 34 \cdot 1973$ and use the Descent Procedure to write the prime 1973 as a sum of two squares.

> To perform this computation, we use the `descent` program developed in the next exercise. Here, `descent(259,1,1973)` returns `(-23,38)`. So
> $$1973 = (-23)^2 + 38^2.$$

(b) Start from $261^2 + 947^2 = 10 \cdot 96493$ and use the Descent Procedure to write the prime 96493 as a sum of two squares.

> To perform this computation, we use the `descent` program developed in the next exercise. Here, `descent(261,947,96493)` returns `(-258,-173)`. So
> $$96493 = (-258)^2 + (-173)^2.$$

E. Silverman 24.8. Write a program that solves $x^2 + y^2 = n$ by trying $x = 0, 1, 2, 3, \ldots$ and checking if $n - x^2$ is a perfect square. Your program should return all solutions with $x \leqslant y$ if any exist and should return an appropriate message if there is no solution.

```
def descent(A, B, p):
    "return integers (A,B) s.t. A^2+B^2=p; p prime congruent to 1
        mod 4, via Fermat's descent method"
    M = ((A ** 2) + (B ** 2)) // p
    if ((A ** 2) + (B ** 2)) % p != 0:
        return "No solution exists."
    else:
        while M > 1:
            u = A % M
            while u > (M // 2):
                u = u - M
            v = B % M
            while v > (M // 2):
                v = v - M
            A, B = ((u * A) + (v * B)) // M, ((v * A) - (u * B)) //
                M
            M = ((A ** 2) + (B ** 2)) // p
        return A, B
```

Proof. Let A_i, B_i, and M_i be the respective values of the python variables `A`, `B`, and `M` after the i^{th} iteration of the program, and let p be the fixed value of the parameter p. Let u_{i_j} and v_{i_k} be respective values of the variables `u` and `v` after the $i_j{}^{th}$ and $i_k{}^{th}$ iterations of their respective inner `while` loops. Note that $A_0, B_0 \in \mathbb{Z}$ and $p \in \mathbb{Z}_{>0}$, so $M_0 = \lfloor \frac{A_0 + B_0^2}{p} \rfloor \in \mathbb{Z}_{>0}$. Fix i. Then since $u_{i_j} = u_{i_{j-1}} - M_i$ and $v_{i_k} = v_{i_{k-1}} - M_{i-1}$ at j^{th} and k^{th} iterations of their respective `while` loops, it is clear that there is r, s such that $u_{i_r} \leqslant \lfloor \frac{M_i}{2} \rfloor$ and $v_{i_s} \leqslant \lfloor \frac{M_i}{2} \rfloor$. Similarly, at each iteration i, $M_i = \lfloor \frac{A_{i-1}^2 + B_{i-1}^2}{p} \rfloor$, so $\{M_i\}$ is a decreasing sequence of positive integers. Thus there exist k in the domain of the sequence $\{M_i\}$ such that $M_k \leqslant 1$. This concludes the proof of termination. Proof of correctness follows from discussion in Silverman (pg. 185-87). ∎

F. Recall that $D_m = \{ d \in \mathbb{N} : d \mid m \}$. Use the Fundamental Theorem of Arithmetic to show that if $\gcd(m, n) = 1$, then the map

$$\begin{aligned} D_m \times D_n &\to D_{mn} \\ (d, e) &\mapsto de \end{aligned}$$

is a bijection.

G. 27.1. A function $f(n)$ that satisfies the multiplication formula

$$f(mn) = f(m)f(n) \quad \text{for all numbers } m \text{ and } n \text{ with } \gcd(m, n) = 1$$

is called a *multiplicative function*.

Suppose now that $f(n)$ is any multiplicative function, and define a new function

$$g(n) = f(d_1)+f(d_2)+\ldots+f(d_r), \quad \text{where } d_1, d_2, \ldots, d_r \text{ are all divisors of } n.$$

Prove that $g(n)$ is a multiplicative function.

Proof. Assume $\gcd(m, n) = 1$ for some $m, n \in \mathbb{Z}$. By the previous exercise, any divisor d of mn can be written uniquely as $d = ek$, where $e \mid m$ and $k \mid n$. So

$$g(mn) = \sum_{d \mid mn} f(d) = \sum_{e \mid m, k \mid n} f(ek).$$

But since $\gcd(m, n) = 1$, it follows that $\gcd(e, k) = 1$. Therefore, by hypothesis,

$$\sum_{e \mid m, k \mid n} f(ek) = \sum_{e \mid m, k \mid n} f(e)f(k) = \sum_{e \mid d} f(e) \sum_{k \mid n} f(k) = g(m)g(n).$$

■