15 Number Theory

15.6 Computing roots Modulo p

CATAM coursework for Part II of the Mathematical Tripos. Sections have been numbered as they appear in the manual.

2 Computing Legendre Symbols

Question 1 We implement the repeated squaring method for modular exponentiation using a recursive algorithm:

$$a^n \equiv \begin{cases} (a^{\frac{n}{2}})^2, & n \text{ even}, n > 0 \\ a \cdot (a^{\frac{n-1}{2}})^2, & n \text{ odd} \\ 1, & n = 0 \end{cases} \pmod{p}$$

This allows for efficient application of Euler's criterion to compute Legendre symbols. For $p = 30275233$, we compute (a/p) for a taking:

(i) 100 random values between 1 and p. Out of these, ?? numbers were found to be quadratic residues mod p.

(ii) all values between 1 and 100. Out of these, 58 numbers were found to be quadratic residues mod p.

Appendix A contains a record of all output produced.

Question 2 Suppose n is any odd number and $m \in \mathbb{Z}$. If $n = 1$, we have $(m/n) = (m/1) = 1$. Otherwise, we may assume $0 \leq m < n$ by reducing mod n if necessary. Note that $(0/n) = 0$ when $n > 1$. If m is a non-zero even number, we may get rid of all factors of 2 using the following property of the Jacobi symbol:

Lemma For any positive odd n we have

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8} = \begin{cases} +1, & n \equiv \pm 1 \pmod 8 \\ -1, & n \equiv \pm 3 \pmod 8 \end{cases}$$

A proof of this can be found in [1] (*pp.* 47, Proposition II.2.6). Hence we

may assume m, n are both odd and $1 \leq m < n$. We state the following strengthening of quadratic reciprocity:

Lemma For any two positive odd integers m and n we have

$$\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4} \left(\frac{n}{m}\right).$$

A proof of this can be found in [1] (*pp.* 47, Proposition II.2.7), but it follows immediately from the law of quadratic reciprocity and the observation that $(m/n) = 0$ whenever m and n are not coprime. Moreover, we can avoid computing the large product $(m-1)(n-1)/4$ by observing that

$$(-1)^{(m-1)(n-1)/4} = \begin{cases} -1, & m, n \equiv 3 \pmod 4 \\ +1, & \text{otherwise} \end{cases}$$

To compute (m/n), it now suffices to compute (n/m). Note that the 'denominator' strictly decreases after each iteration, hence the recursion must halt in finite time.

COMPLEXITYCOMPLEXITYCOMPLEXITY

3 Computing square roots mod p

Question 3 Suppose $p \equiv 3 \pmod 4$ and a is a residue mod p. In particular, Euler's criterion implies $a^{(p-1)/2} \equiv 1 \pmod p$. Then $x \equiv a^{(p+1)/4}$ is a solution to $x^2 \equiv a \pmod p$ since

$$x^2 \equiv a^{(p+1)/2} \equiv a \cdot a^{(p-1)/2} \equiv a \pmod p.$$

Suppose $p \equiv 5 \pmod 8$. We have $(2/p) \equiv 2^{(p-1)/2} \equiv -1 \pmod p$. If a is a quadratic residue, we have $a^{(p-1)/2} \equiv 1 \Rightarrow a^{(p-1)/4} \equiv \pm 1 \pmod p$. In particular, we can write $2^{k(p-1)/2} \cdot a^{(p-1)/4} \equiv 1 \pmod p$ for some $k \in \{0, 1\}$. But then we have $a \equiv 2^{k(p-1)/2} \cdot a^{(p-1)/4} \cdot a \equiv 2^{k(p-1)/2} \cdot a^{(p+3)/4} \pmod p$. Observe that all the exponents involved are even, so we can read off a solution to $x^2 \equiv a$ as $x \equiv 2^{k(p-1)/4} \cdot a^{(p+3)/8} \pmod p$.

Now suppose p is a prime of the form $2^n + 1$ (we only consider $n > 2$ since $p = 3, 5$ have been covered above). Then $p \equiv (-1)^n + 1 \pmod 3$, hence

n must be even. It follows that $p \equiv 1 \pmod 4$ and $p \equiv 2 \pmod 3$, so that $(3/p) = (p/3) = (2/3) = -1$. Let g be any primitive root mod p. The subgroup $\langle g^2 \rangle$ has order $2^{n-1} = \frac{p-1}{2}$ hence contains all the quadratic residues. Moreover, it is the unique multiplicative subgroup of order 2^{n-1}. Since $3 \notin \langle g^2 \rangle$, the multiplicative order of 3 must be 2^n i.e. 3 is also a primitive root mod p.

Question 4 Suppose $p = 65537 = 2^{16} + 1$, and we wish to solve the congruence $x^2 \equiv 18612 \pmod p$. We compute $(18612/65537) = 1$ using the program written for Question 2, so such an x exists. For the purposes of this question, use '=' to denote congruence mod p. For modular exponentiation, we use a program based on the repeated squaring method.

Since 3 is a primitive root mod p, we may write $x = 3^{r_0 + 2r_1 + 2^2 r_2 + \cdots}$ where each $r_j \in \{0, 1\}$. The congruence $x^2 = 18612$ can be written as $\prod_{j \geq 0} 3^{r_j 2^{j+1}} = 18612 \pmod p$.

Raising both the sides to 2^{14}, all the terms for $j \geq 1$ vanish and we are left with $3^{r_0 2^{15}} = 18612^{2^{14}} = 1$. Since 3 is a primitive root, $3^{2^{15}} = -1$ by Euler's criterion and we have $r_0 = 0$. In fact, $18612^{2^n} = 1$ for all $14 \geq n \geq 11$ hence we have $r_0 = ... = r_3 = 0$.

Raising both the sides of $\prod_{j \geq 4} 3^{r_j 2^{j+1}} = 18612$ to the power 2^{10}, we obtain $3^{r_4 2^{15}} = -1$, hence $r_4 = 1$. We may multiply both the sides of the congruence by $3^{-r_4 2^5} = 3^{2^{16} - 2^5} = 29606$ to obtain $\prod_{j \geq 5} 3^{r_j 2^{j+1}} = 57313$.

Again, $57313^{2^n} = 1$ for $9 \geq n \geq 6$, so $r_5 = ... = r_8 = 0$, and we have $\sum_{j \geq 9} 3^{r_j 2^{j+1}} = 57313$. Raising both the sides to the power 2^5, we obtain $3^{r_9 2^{15}} = -1$, hence $r_9 = 1$. Multiply both the sides by $3^{-r_9 2^{10}} = 3^{2^{16} - 2^{10}} = 64509$ to obtain $\prod_{j \geq 10} 3^{r_j 2^j} = 65536 = -1$. Comparing with $3^{2^{15}} = -1$, we deduce $r_{10} = ... = r_{13} = 0$ and $r_{14} = 1$.

We can now read off the solution to $x^2 = 18612$ as $x = 3^r$ where $r = 2^4 + 2^9 + 2^{14}$. A square root of 18612 (mod p) hence is 45462. The other square root is $-45462 = 20075$ and these are the only solutions to $x^2 = 18612$ since $(\mathbb{Z}/p\mathbb{Z})^*$ is a field.

Suppose p is any odd prime and a is a quadratic residue mod p. In this section, use '=' to denote congruence mod p. We may find $\alpha > 0$ and s odd

such that $p - 1 = 2^\alpha s$. Since s is odd, we define $z = a^{(s+1)/2}$ and observe that if $y^2 = a^s$, then zy^{-1} is a square root of a mod p (where y^{-1} is the multiplicative inverse of y in $(\mathbb{Z}/p\mathbb{Z})^\times$.)

Now $(a^s)^{2^{\alpha-1}} = a^{(p-1)/2} = (a/p) = 1$, so y is an element of the cyclic multiplicative group $G = \{g \in (\mathbb{Z}/p\mathbb{Z})^\times \mid g^{2^\alpha} = 1\}$. Suppose n is any non-residue mod p, and let $b = n^s$. Then we have $b^{2^\alpha} = n^{p-1} = 1$ hence $b \in G$, and moreover b generates the group since $b^{2^{\alpha-1}} = n^{(p-1)/2} = (n/p) = -1$. We can then write $y = b^r$, and solve for r algorithmically by considering its binary expansion. A square root of a, then, is $zb^{2^\alpha - r}$.

Question 5 We implement an algorithm that uses the above method to compute square roots mod p when $p \equiv 1 \pmod 8$, using the more direct computations from Question 3 to handle other cases. The second solution to the congruence $x^2 \equiv a \pmod p$ can be computed as -1 times the first solution.

Here are some test cases, in the form `(a, root a)`. The values of a (other than the first) have been chosen randomly subject to being quadratic residues. The primes have been chosen[1] to cover all possible congruence classes mod 8. The generated roots can be confirmed to be accurate by squaring them. In particular, the first test case agrees with what we found in Question 4.

```
mod 65537:   (18612, 45462)  (29495, 60940)  (5923, 59157)
mod 10501:   (9679, 5433)    (8170, 7049)    (6120, 5603)
mod 10601:   (6155, 865)     (6141, 3706)    (3597, 1877)
mod 11311:   (9583, 2771)    (10615, 1240)   (5763, 3891)
mod 11411:   (11163, 8293)   (7172, 5189)    (5120, 10477)
```

Additionally, we compute the roots of all quadratic residues in $\{1, 2, ..., 20\}$ mod 30275233 and present the results in Appendix B.

COMPLEXITYCOMPLEXITYCOMPLEXITY

4 Computing roots of polynomials mod p

Let p be a prime.

Question 6 Given two polynomials f and g in $(\mathbb{Z}/p\mathbb{Z})[x]$, note that $\mathbb{Z}/p\mathbb{Z}$

[1]The first prime is the largest known Fermat prime, while the latter four are relatively large palindromic primes [OEIS: A055578].

is a field hence the leading coefficient of g is a unit– moreover, we can use Fermat's little theorem to explicitly compute its inverse using the repeated squaring method. With this, we implement a recursive algorithm to eliminate terms in f of degree higher than $\deg(g)$ and find polynomials q, r such that $f = qg + r$, $\deg(r) < \deg(g)$. Write $r = \mathrm{rem}(f, g)$.

This allows for the application of Euclid's algorithm to find the greatest common divisor of f and g, by

$$\gcd(f, g) = \begin{cases} f, & g = 0 \\ \gcd(g, \mathrm{rem}(f, g)), & \text{otherwise} \end{cases}.$$

The answer is generated up to a unit, so we divide by the leading coefficient to normalise. To test the algorithm, we compute the greatest common divisors for the following pairs of polynomials:

$$\begin{aligned} &\gcd(x^3 + 6x^2 + 5x + 5, x^3 + 13x^2 + 6x + 3) = x^2 + 78x + 62 && (p = 109). \\ &\gcd(x^3 + 2x^2 + 9x + 4, x^3 + 3x^2 + 7x + 9) = 1 && (p = 131). \\ &\gcd(x^3 + 3x^2 + 9x + 12, x^3 + 6x^2 + 12x + 4) = x + 83 && (p = 157). \end{aligned}$$

If f, g, h are polynomials, write $f \equiv g \pmod{h}$ to mean 'there exists a polynomial q such that $f = qh + g$.' It is straightforward to check that this is an equivalence relation, and $f_1 \equiv g_1 \pmod{h}$, $f_2 \equiv g_2 \pmod{h}$ implies $f_1 + f_2 \equiv g_1 + g_2 \pmod{h}$ and $f_1 f_2 \equiv g_1 g_2 \pmod{h}$. Moreover, $\mathrm{rem}(f, h)$ is the unique g such that $f \equiv g \pmod{h}$, $\deg(g) < \deg(h)$. It follows that $f \equiv f' \pmod{h}$ implies $\mathrm{rem}(f, h) = \mathrm{rem}(f', h)$.

Let $f \in (\mathbb{Z}/p\mathbb{Z})[x]$ be any polynomial. The polynomial $\Phi(x) = x^p - x$ factorises as $\Phi(x) = \prod_{i=0}^{p-1}(x - i)$ hence $g = \gcd(f, \Phi)$ is a product of distinct linear factors. Moreover, $(x - i) \mid f$ if and only if $(x - i) \mid g$, hence to compute the roots of f it suffices to compute the roots of g.

Now the computation of g using Euclidean algorithm takes at most $\deg(f)$ steps, and in each step except for the first one, the degree of polynomials involved is less than $\deg(f)$. Naively computing $\mathrm{rem}(\Phi, f)$ would take $O(p)$ steps; however we observe that

$$\mathrm{rem}(x^p - x, f) \equiv \mathrm{rem}(x^p, f) - \mathrm{rem}(x, f) \pmod{h}$$

The second term is straightforward to compute. For the first term, we can use a repeated squaring algorithm similar to that for modular exponentiation of numbers. This speeds up the first step of Euclidean algorithm to take $O(\log p)$ steps, and moreover the polynomials involved in each computation have degree at most $2\deg(f)$.

Having reduced f to the case where it is a product of distinct linear factors, we fix a $v \in \mathbb{Z}/p\mathbb{Z}$ and compute $\gcd((x+v)^{(p-1)/2} - 1, f)$. Everything that has been said about avoiding large powers in the computation applies here. The greatest common divisor is f if $\alpha + v$ is a quadratic residue for every root α of f, it is 1 if $\alpha + v$ is a non-residue for every root α of f. Otherwise, we have arrived at a non-trivial factor of f, and can repeat the process with these till we have found all linear factors (and hence the roots).

Appendix A: Computed Legendre symbols

Using Euler's criterion, Legendre symbols were computed for 100 random values between 1 and $p = 30275233$. The results are recorded here in the format `a: (a/p)`.

```
24644851:  1     11967300: -1      1445474: -1     14007048:  1
 4717325: -1     24478989: -1      8624473: -1     14317196: -1
29167052: -1      1233462:  1     15720323: -1     27049206: -1
 1096707:  1      7374707:  1     12630188: -1     10163177:  1
27701652:  1      7504160: -1     12174675:  1      5744228: -1
23557225: -1       611555: -1     13518518:  1     18159019: -1
17475596: -1     13586647: -1     21475751:  1     10251437: -1
14667247: -1     11711873: -1      7830360: -1     24610743:  1
11975600:  1     20544717:  1     29906048:  1     17985135: -1
 4343490: -1       595770:  1     10029144: -1     23426589:  1
 6826173: -1     15252287: -1     12186080:  1     24535554: -1
 7951147: -1     22571565: -1      3880370:  1     17379741:  1
 2885585: -1     11457354:  1     19765043: -1     21579652:  1
10802437:  1      7656736:  1      3031411:  1      5571495:  1
 2961952:  1     25581914: -1     20059655:  1      4451766:  1
 9799989: -1     24023211: -1     20737189:  1     13632361: -1
 3657503: -1     26898118: -1     11789779:  1     20320034: -1
  806166: -1     16756478: -1      1626490: -1     19052907: -1
 7768803: -1     17909369: -1       523714: -1     17796937: -1
```

```
15739391: -1     10355715: -1     21536538:  1     24904705:  1
12096136:  1     15769909: -1     28314425:  1      1797884: -1
19918249: -1      5237282:  1     22563315:  1     27068694: -1
 2739165:  1     30266523: -1     11315725: -1     14166899: -1
27441661:  1      1253064:  1     20874181: -1     10807494: -1
16534851:  1     24731354: -1     25694393:  1      9865287:  1
```

```
Number of quadratic residues encountered: 42
```

We also perform a similar calculation for all a between 1 and 100.

```
  1:  1       2:  1       3:  1       4:  1       5: -1
  6:  1       7:  1       8:  1       9:  1      10: -1
 11: -1      12:  1      13:  1      14:  1      15: -1
 16:  1      17:  1      18:  1      19:  1      20: -1
 21:  1      22: -1      23: -1      24:  1      25:  1
 26:  1      27:  1      28:  1      29:  1      30: -1
 31: -1      32:  1      33: -1      34:  1      35: -1
 36:  1      37: -1      38:  1      39:  1      40: -1
 41: -1      42:  1      43: -1      44: -1      45: -1
 46: -1      47:  1      48:  1      49:  1      50:  1
 51:  1      52:  1      53:  1      54:  1      55:  1
 56:  1      57:  1      58:  1      59: -1      60: -1
 61: -1      62: -1      63:  1      64:  1      65: -1
 66: -1      67:  1      68:  1      69: -1      70: -1
 71: -1      72:  1      73:  1      74: -1      75:  1
 76:  1      77: -1      78:  1      79: -1      80: -1
 81:  1      82: -1      83:  1      84:  1      85: -1
 86: -1      87:  1      88: -1      89: -1      90: -1
 91:  1      92: -1      93: -1      94:  1      95: -1
 96:  1      97: -1      98:  1      99: -1     100:  1
```

```
Number of quadratic residues encountered: 58
```

Appendix B: Roots of residues mod 30275233

For every integer $1 \leq a \leq 20$, we check if a is a quadratic residue mod $p = 30275233$ and if so, compute a solution to $x^2 \equiv a \pmod{p}$. The computed roots are presented in format `(a, root a)`.

```
(1, 1)           (2, 1149953)     (3, 2513663)
(4, 2)           (6, 5886698)     (7, 2907008)
(8, 2299906)     (9, 3)           (12, 5027326)
(13, 11851235)   (14, 22168463)   (16, 30275229)
(17, 18030218)   (18, 3449859)    (19, 4272041)
```

References

[1] Koblitz, N. *A course in Number Theory and Cryptography*, Graduate Texts in Mathematics 114, Springer, 1987.