2 Discrete logarithms

Primitive roots

Exercise 2.1. Let p be an odd prime, and let $k \geqslant 1$ be an integer. Consider the sum

$$S_k = 1^k + 2^k + \cdots + (p-1)^k.$$

(a) Prove that $S_{p-1} \equiv -1 \mod p$.

(b) Prove that if $p - 1 \nmid k$, then $S_k \equiv 0 \mod p$.

Exercise 2.2. Prove that if g is a primitive root modulo m, then

$$a \equiv b \pmod{\phi(m)} \iff g^a \equiv g^b \pmod{m}.$$

Solving congruences

Exercise 2.3. Fix a positive integer m and integers a, b.

(a) Prove that for all nonzero integers d we have: $a \equiv b \pmod{m}$ if and only if $da \equiv db \pmod{dm}$.

(b) Prove that if $d \nmid b$ then $da \not\equiv b \pmod{dm}$.

Exercise 2.4. Solve the congruences:

(a) $8x \equiv 7 \pmod{43}$.

(b) $x^8 \equiv 17 \pmod{43}$.

(c) $8^x \equiv 3 \pmod{43}$.

Use the fact that 3 is a primitive root modulo 43, and the following values of the discrete logarithm in base 3:

$$\log_3(7) = 35 \qquad \log_3(8) = 39$$
$$\log_3(17) = 38 \qquad \log_3(3) = 1.$$

Exercise 2.5. Solve the following congruences using discrete logarithms:

(a) $16x \equiv 14 \pmod{82}$.

(b) $(2x)^3 \equiv 34 \pmod{50}$.

(c) $11 \cdot (3x)^2 \equiv 63 \pmod{162}$.

(d) $8^x \equiv 46 \pmod{82}$.

[**Hint**: 7 is a primitive root modulo 41, 2 is a primitive root modulo 25, and 5 is a primitive root modulo 18.]

Primitive roots modulo prime powers

Exercise 2.6. Let p be an odd prime number and let g be a primitive root modulo p.

(a) Prove that, as an element of the group $(\mathbf{Z}/p^2\mathbf{Z})^\times$, g has order $p-1$ or order $p(p-1)$.

(b) Using part (a), prove that either g or $g+p$ is a primitive root modulo p^2 (that is, a generator of the group $(\mathbf{Z}/p^2\mathbf{Z})^\times$).

[**Hint**: Expand $(g+p)^{p-1}$ using the Binomial Theorem.]

Exercise 2.7. Let p be an odd prime number and let g be a primitive root modulo p^2.

(a) Prove that $g^{p-1} = 1 + ap$ for some integer a such that $p \nmid a$.

(b) Prove that g is a primitive root modulo p^3.

[**Hint**: Use part (a) and inspiration from Exercise 2.6.]

(Induction based on the above argument can be used to prove that g is a primitive root modulo p^k for all $k \geqslant 2$.)

Exercise 2.8. Let p be an odd prime and $k \in \mathbf{Z}_{\geqslant 1}$.

Suppose g is a primitive root modulo p^k. Show that $\log_g(-1) = \dfrac{\phi(p^k)}{2}$.
Use this to solve the following congruence:

$$x^2 \equiv -1 \pmod{91^3}.$$

Quadratic residues

Exercise 2.9. Use quadratic reciprocity to show that if p is an odd prime, then

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{1)2} \\ -1 & \text{if } p \equiv \pm 5 \pmod{1)2}. \end{cases}$$

Find a similar formula for $\left(\dfrac{-3}{p}\right)$. Why is the second one simpler?

Exercise 2.10 (Quadratic residues modulo p^2)**.**

(a) Find the quadratic residues modulo 9.

(b) How many quadratic residues do you expect to see modulo p^2 for an odd prime p?

Try to prove this by mimicking the proof of Proposition 2.6 and Tutorial Question 5.1.

Exercise 2.11. Suppose a prime p is a sum of three squares. Prove that $p \not\equiv 7 \pmod 8$.

Exercise 2.12. Consider prime numbers p that can be written as the difference of two positive integer cubes:

$$p = x^3 - y^3, \qquad x, y \in \mathbf{Z}_{\geqslant 1}.$$

(a) Prove that a prime p is can be written as a difference of two positive integer cubes if and only if $p = 3y^2 + 3y + 1$ for some $y \in \mathbf{Z}_{\geqslant 1}$.

(b) Find all such primes < 100.

(c) Prove that such prime p satisfies $p \equiv 1, 7 \pmod 9$.

(It is an unsolved conjecture that there are infinitely many such primes.)

Answers

Solution 2.1.

(a) Apply Fermat's little Theorem:

$$S_{p-1} = 1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv 1 + 1 + \cdots + 1 = p - 1 \equiv -1 \pmod{p}.$$

(b) Suppose that g is a primitive root modulo p, then we know that every integer coprime to p is congruent to g^r modulo p for some unique integer $0 \leqslant r < p-1$. Then

$$S_k = 1^k + 2^k + \cdots + (p-1)^k = \sum_{i=1}^{p-1} g^{ik}. \tag{1}$$

Since $(p-1) \nmid k$, we have:

$$g^k \not\equiv 1 \pmod{p}.$$

Let us multiply (1) by g^k:

$$g^k S_k = \sum_{i=1}^{p-1} g^{ik+k} = \sum_{i=1}^{p-1} g^{(i+1)k} = \sum_{j=2}^{p} g^{jk}.$$

I claim that $g^k S_k \equiv S_k \pmod{p}$. To see this, first note that $g^k S_k - S_k = g^{pk} - g^k$ because all other summation terms cancel out. Now

$$g^{pk} \equiv (g^p)^k \equiv g^k \pmod{p},$$

since $g^{p-1} \equiv 1 \pmod{p}$ by Fermat's little Theorem. Hence

$$g^k S_k \equiv S_k \pmod{p},$$

which implies:

$$(g^k - 1) S_k \equiv 0 \pmod{p}.$$

Since $g^k - 1 \not\equiv 0 \mod p$, and p is prime, we conclude that $S_k \equiv 0 \pmod{p}$.

Solution 2.2. Suppose, without loss of generality, that $a \leqslant b$. Since g is a primitive root modulo m we know, in particular, that it has a modulo m inverse. So we may cancel a copies of g to show that $g^a \equiv g^b \pmod{m}$ if and only if $1 \equiv g^{b-a} \pmod{m}$. That in turn is the case if and only if the order of g divides $b - a$. However, the order of g is $\phi(m)$ since g is a primitive root modulo m.

Hence the last condition holds if and only if $a \equiv b \pmod{\phi(m)}$.

Solution 2.3.

(a) Suppose $a \equiv b \pmod{m}$, then there exists $k \in \mathbf{Z}$ such that $a - b = km$. Then $da - db = kdm$, so $da \equiv db \pmod{dm}$.

Conversely, if $da \equiv db \pmod{dm}$ then there exists $k \in \mathbf{Z}$ such that $d(a-b) = d(km)$. Since d is nonzero we can divide it out on both sides to get $a - b = km$, so $a \equiv b \pmod{m}$.

(b) We prove the contrapositive. Suppose $da \equiv b \pmod{dm}$, then there exists $k \in \mathbf{Z}$ such that $da - b = kdm$. Therefore $b = da - kdm = d(a - km)$, so d divides b.

Solution 2.4.

(a) We have $\log_3(8) + \log_3(x) \equiv \log_3(7) \pmod{42}$, so $39 + \log_3(x) \equiv 35 \pmod{42}$, so $\log_3(x) \equiv 38 \pmod{42}$, so $x \equiv 3^{38} \equiv 17 \pmod{43}$.

(b) We have $8\log_3(x) \equiv \log_3(17) \equiv 38 \pmod{42}$. Dividing through by 2 we have $4\log_3(x) \equiv 19 \pmod{21}$. Since 4 is invertible modulo 21 with inverse -5, we get $\log_3(x) \equiv (-5) \cdot 19 \equiv 10 \pmod{21}$.

We should bring this back modulo 42 before exponentiating: $\log_3(x) \equiv 10, 31 \pmod{42}$. Therefore $x \equiv 3^{10}, 3^{31} \equiv 10, 33 \pmod{43}$.

(c) We have $x\log_3(8) \equiv 1 \pmod{42}$, so $39x \equiv 1 \pmod{42}$, impossible since 3 divides both 39 and 42, but not 1.

So the congruence has no solutions.

Solution 2.5.

(a) Using Exercise 2.3 we have

$$16x \equiv 14 \pmod{82}$$

if and only if

$$8x \equiv 7 \pmod{41}.$$

Taking discrete logarithms with respect to the primitive root 7, we get

$$\log_7(8x) \equiv \log_7(7) \equiv 1 \pmod{40}.$$

Using properties of the discrete logarithm we get

$$\log_7(8) + \log_7(x) \equiv 1 \pmod{40} \quad \Rightarrow \quad \log_7(x) \equiv 1 - \log_7(8) \equiv \log_7(7/8) \pmod{40}.$$

We now take the inverse of $\log_7$:

$$x \equiv 7/8 \equiv 7 \cdot 36 \equiv 6 \pmod{41}.$$

We conclude that the solutions of the original congruence are all integers x that are congruent to 6 modulo 41.

(b) Similar to part (a), using logarithms in base 2. Arrive at

$$\log_2(x) \equiv 7\log_2(17/4) \equiv 20,$$

therefore

$$x \equiv (17/4)^7 \equiv (17 \cdot (-6))^7 \equiv (-2)^7 \equiv -32 \cdot 4 \equiv 22 \pmod{25}.$$

(c) We start similarly to the previous parts, after dividing through by 9 and taking logarithms in base 5:

$$\log_5(11x^2) \equiv \log_5(7) \pmod 6.$$

From here we get to

$$2\log_5(x) \equiv \log_5(7/11) \equiv \log_5(7 \cdot 5) \equiv \log_5(-1) \pmod 6.$$

But 5 is a primitive root modulo 18, so $5^6 = 1$, so $5^3 = -1$, in other words $\log_5(-1) = 3$. Placing this back in the last congruence:

$$2\log_5(x) \equiv 3 \pmod 6,$$

we realise that this is unsolvable since 2 divides $2\log_5(x)$ and 6, but not 3.

Therefore the original congruence has no integer solutions.

(d) Divide through by 2 to get

$$4 \cdot 8^{x-1} \equiv 23 \pmod{41} \quad \Rightarrow \quad 8^{x-1} \equiv -230 \equiv 16 \pmod{41}.$$

Taking logarithms in base 7:

$$3(x-1)\log_7(2) \equiv 4\log_7(2) \pmod{40} \quad \Rightarrow \quad (3x-7)\log_7(2) \equiv 0 \pmod{40}.$$

At this point we need to find out (for instance by brute force) that $\log_7(2) = 14$. We get

$$14(3x-7) \equiv 0 \pmod{40} \Rightarrow 7(3x-7) \equiv 0 \pmod{20} \Rightarrow 3x-7 \equiv 0 \pmod{20} \Rightarrow x \equiv 9 \pmod{20}$$

Solution 2.6.

(a) Let n be the order of g in $(\mathbf{Z}/p^2\mathbf{Z})^\times$.

Then n divides the cardinality of the group, which is $\phi(p^2) = p(p-1)$.

On the other hand, we have $g^n \equiv 1 \pmod{p^2}$, which implies that $g^n \equiv 1 \pmod p$. Since g is a primitive root modulo p, its order in $(\mathbf{Z}/p\mathbf{Z})^\times$ is $p-1$, hence $(p-1) \mid n$.

Putting together $(p-1) \mid n \mid p(p-1)$, we conclude that $n = p-1$ or $n = p(p-1)$.

(b) First note that since $g + p \equiv g \pmod p$, $g+p$ is also a primitive root modulo p.

If g is a primitive root modulo p^2, we are done. So suppose g is not a primitive root modulo p^2. We will prove that $g+p$ is.

By part (a), the order of g as an element of $(\mathbf{Z}/p^2\mathbf{Z})^\times$ is $p-1$. Also using part (a), if we prove that

$$(g+p)^{p-1} \not\equiv 1 \pmod{p^2},$$

then $g+p$ does not have order $p-1$, hence must have order $p(p-1)$ and be a primitive root modulo p^2.

To prove the above non-congruence, we use the Binomial Theorem:

$$\begin{aligned}(g+p)^{p-1} &= g^{p-1} + (p-1)pg^{p-2} + \binom{p-1}{2}p^2g^{p-3} + \cdots + (p-1)p^{p-2}g + p^{p-1} \\ &\equiv g^{p-1} + (p-1)pg^{p-2} \equiv g^{p-1} - pg^{p-2} \equiv 1 - pg^{p-2} \not\equiv 1 \pmod{p^2},\end{aligned}$$

where for the last step we used the fact that $p \nmid g$ so $pg^{p-2} \not\equiv 0 \pmod{p^2}$.

Solution 2.7.

(a) We have $g^{p-1} \equiv 1 \pmod{p}$ by Fermat's little Theorem, but $g^{p-1} \not\equiv 1 \pmod{p^2}$ (since g is a primitive root modulo p^2, hence its order is $p(p-1)$).

Therefore, writing $ap = g^{p-1} - 1$, we have that $p \nmid a$.

(b) Let n be the order of g in $(\mathbf{Z}/p^3\mathbf{Z})^\times$. Then $n \mid p^2(p-1)$.

But also, since $g^n \equiv 1 \pmod{p^3}$, we have $g^n \equiv 1 \pmod{p^2}$, so $p(p-1) \mid n$.

From $p(p-1) \mid n \mid p^2(p-1)$ we deduce that $n = p(p-1)$ or $p^2(p-1)$.

It remains to prove that $n \neq p(p-1)$:

$$\begin{aligned}g^{p(p-1)} = (g^{p-1})^p = (1+ap)^p &= 1 + pap + \binom{p}{2}a^2p^2 + \binom{p}{3}a^3p^3 + \cdots + a^pp^p \\ &\equiv 1 + ap^2 \not\equiv 1 \pmod{p^3}.\end{aligned}$$

Here we used the fact that $\binom{p}{2}$ is divisible by p, so that $\binom{p}{2}a^2p^2 \equiv 0 \pmod{p^3}$, and finally the fact that $p \nmid a$.

Solution 2.8. Let $e = \log_g(-1)$. We have $g^e \equiv -1 \pmod{p^k}$, so $g^{2e} \equiv 1 \pmod{p^k}$, so $\phi(p^k) \mid 2e$. Since p is odd, $\phi(p^k) = p^{k-1}(p-1)$ is even, so $\phi(p^k) \mid 2e$ if and only if $(\phi(p^k)/2) \mid e$.

On the other hand, certainly e satisfies $0 \leqslant e < \phi(p^k)$, so we are left with the possibilities $e = 0$ or $e = \phi(p^k)/2$. For $e = 0$ we would have $-1 \equiv g^0 \equiv 1 \pmod{p^k}$, certainly not the case unless $p^k = 2$.

Now for the congruence.

The modulus 91^3 is divisible by 7, so if a is a solution to $x^2 \equiv -1 \pmod{91^3}$ then it is also a solution to $x^2 \equiv -1 \pmod{7}$.

As 7 is small, we can check directly that the latter congruence has no solutions, or we can take discrete logarithms with respect to some primitive root g modulo 7:

$$2\log_g(x) \equiv \log_g(-1) \equiv \phi(7)/2 \equiv 3 \pmod{6},$$

where we applied the fact at the top. This congruence is unsolvable since 2 divides the left hand side and the modulus, but not the right hand side.

Therefore the original congruence also has no solutions.

Solution 2.9. Applying quadratic reciprocity, we see that

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & \text{if } p \equiv 1 \pmod 4, \text{ and} \\ -\left(\frac{p}{3}\right) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Now to compute the Legendre symbols on the right we reduce p modulo 3 and observe that

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1 & \text{if } p \equiv 1 \pmod 3, \text{ and} \\ \left(\frac{2}{3}\right) = -1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

To combine everything into a single statement, we observe that the given conditions involve congruences modulo 4 and 3 respectively and so we may classify the four possibilities here by examining the four possible values $1, 5, 7$, and 11 of $p \mod 12$.

$$\begin{aligned}
p \equiv 1 \pmod{12} &\implies p \equiv 1 \pmod 4 \text{ and } p \equiv 1 \pmod 3 \implies \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1 \\
p \equiv 5 \pmod{12} &\implies p \equiv 1 \pmod 4 \text{ and } p \equiv 2 \pmod 3 \implies \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = -1 \\
p \equiv 7 \pmod{12} &\implies p \equiv 3 \pmod 4 \text{ and } p \equiv 1 \pmod 3 \implies \left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -1 \\
p \equiv 11 \pmod{12} &\implies p \equiv 3 \pmod 4 \text{ and } p \equiv 2 \pmod 3 \implies \left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = 1.
\end{aligned}$$

To compute $\left(\frac{-3}{p}\right)$ we observe that it is equal to $\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$ and we have

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & \text{if } p \equiv 1 \pmod 4 \\ -\left(\frac{p}{3}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases} \qquad \left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

so these signs cancel in each case to simplify our expression to:

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3 \\ -1 & \text{if } p \equiv -1 \pmod 3. \end{cases}$$

Solution 2.10.

(a) Modulo 9, we have $1^2 \equiv 8^2 \equiv 1$, $2^2 \equiv 7^2 \equiv 4$, $4^2 \equiv 5^2 \equiv 7$, so the quadratic residues are $1, 4, 7$.

(b) By Theorem 1.35, the group $(\mathbf{Z}/p^2\mathbf{Z})^\times$ is cyclic of cardinality $p(p-1)$. Therefore there exists a primitive root g modulo p^2. By the same proof as in Proposition 2.6, $a = g^e$ is a quadratic residue if and only if e is even. But $0 \leqslant e < p(p-1)$, so we are counting the number of even integers in this interval: $p(p-1)/2$.

Solution 2.11. Write $p = x^2 + y^2 + z^2$.
Then $p \equiv x^2 + y^2 + z^2 \pmod 8$.
But $x^2 \pmod 8$ can only be one of $\{0, 1, 4\}$.
Therefore the sum of three such numbers can only be one of

$$0+0+0=0, 0+0+1=1, 0+0+4=4, 0+1+1=2, 0+1+4=5,$$
$$0+4+4\equiv 0, 1+1+1=3, 1+1+4=6, 1+4+4\equiv 1, 4+4+4\equiv 4.$$

We conclude that $p \equiv 7 \pmod 8$ is impossible.

Solution 2.12.

(a) If p is such a prime then

$$p = x^3 - y^3 = (x-y)(x^2+xy+y^2).$$

But $x^2 + xy + y^2 \geqslant 3$, so we must have $x - y = 1$, that is $x = y + 1$. Therefore $p = (y+1)^3 - y^3 = 3y^2 + 3y + 1$.

Conversely, we have

$$p = 3y^2 + 3y + 1 = (y+1)^3 - y^3.$$

(b) We try all $y \in \mathbf{Z}_{\geqslant 1}$ such that $3y^2 + 3y + 1 < 100$:

$$\begin{aligned} y = 1 &: \ 3y^2 + 3y + 1 = 7 \\ y = 2 &: \ 3y^2 + 3y + 1 = 19 \\ y = 3 &: \ 3y^2 + 3y + 1 = 37 \\ y = 4 &: \ 3y^2 + 3y + 1 = 61 \\ y = 5 &: \ 3y^2 + 3y + 1 = 91 = 7 \cdot 13, \end{aligned}$$

so the desired primes up to 100 are: $7, 19, 37, 61$.

(c) Simply let y range through $0, 1, \ldots, 8$ and find the corresponding $3y^2 + 3y + 1 \pmod 9$, giving $1, 7, 1, 1, 7, 1, 1, 7, 1$.