

Computing discrete logarithms

MATH2068 Number Theory & Cryptography
Week 11 Lecture 1

University of Sydney
NSW 2006
Australia

8th October 2007



The order of b modulo p

Let p be a prime and b a nonzero residue mod p .

If we compute the mod p residues of b, b^2, b^3 , and so on, then we obtain a periodic sequence.

In other words, there is a number k such that $b^i \equiv b^j \pmod{p}$ whenever i and j differ by a multiple of k .

The smallest such k is called $\text{ord}_p(b)$, the order of b mod p .

Since $\gcd(b, p) = 1$ it follows by coprime cancellation that $b^i \equiv b^j \pmod{p}$ iff $b^{j-i} \equiv 1 \pmod{p}$. So $\text{ord}_p(b)$ is the least $k > 0$ such that $b^k \equiv 1 \pmod{p}$.

We see that $b^m \equiv 1 \pmod{p}$ iff $k|m$. And, as a consequence, $b^i \equiv b^j \pmod{p}$ iff $i \equiv j \pmod{k}$.

Primitive roots and discrete logs



Fermat's Little Theorem guarantees that $b^{p-1} \equiv 1 \pmod{p}$; so $\text{ord}_p(b)$ must be a divisor of $p - 1$.

We say that b is a primitive root mod p if $\text{ord}_p(b) = p - 1$.

We have proved that primitive roots exist: for every prime p there is some b such that $\text{ord}_p(b) = p - 1$.

When b is a primitive root, $b^i \equiv b^j \pmod{p}$ iff $i \equiv j \pmod{p - 1}$.

Thus the mod p residue of b^i does not determine i uniquely, it only determines what i is congruent to modulo $p - 1$.

If $b^i \equiv a \pmod{p}$ then the residue of i modulo $p - 1$ is called the *discrete log of a to the base b* , written $\log_{b,p}(a)$.

The discrete logarithm problem



Suppose that p is a prime and b is a primitive root mod p .

Discrete Logarithm Problem: If a is a positive integer less than p , find k such that $b^k \equiv a \pmod{p}$.

In other words, compute $\log_{b,p}(a)$.

More generally, we would like to be able solve the above problem when b is not necessarily a primitive root, but it is known that a is congruent to some power of p .

Recall that the security of the Elgamal cryptosystem relies on the fact that the Discrete Log Problem is computationally difficult.

The Diffie-Hellman Problem



To be more exact, security of Elgamal relies on the fact that the following problem is computationally difficult:

Diffie-Hellman Problem: Find the mod p residue of b^{xy} given the mod p residues of b^x and b^y .

If one can solve the Discrete Logarithm Problem then one can solve the Diffie-Hellman Problem:

given $b^x \equiv a \pmod{p}$, computing $\log_{b,p}(a)$ gives you the value of $x \pmod{p-1}$, and then you can compute $b^{xy} \equiv (b^y)^x$.

It is believed that there is no better way to solve the Diffie-Hellman problem.

The simple-minded approach



We are given a , and want to find i such that $b^i \equiv a \pmod{p}$.

The most obvious method is to compute the mod p residues of b, b^2, b^3 , etc., until we find one that equals a .

The sequence repeats after $k = \text{ord}_p(b)$ steps; so we either find a solution i that is less than k , or else there is no solution.

This simple-minded approach involves, at worst, computing the residue of b^i for k different values of i .

We would like to be able to do better than this.

Baby-step giant step method



We can reduce the number of values of i for which we compute the residue of b^i from k to $2\sqrt{k}$.

Example: Solve $4^i \equiv 147 \pmod{179}$, given that $\text{ord}_{179}(4) = 89$.

The first step is to find the least M such that $M^2 \geq \text{ord}_p(b)$.

Since $\text{ord}_p(b) = 89$, in fact $M = 10$.

We know that if there is a solution i , there is one with $i < 89$.

Let $i = Mx + y$ with $0 \leq y < M$. Then $x < M$, since $i < M^2$.

We seek $x, y \in \{0, 1, 2, \dots, 9\}$ with $4^{10x+y} \equiv 147 \pmod{179}$.

This can be rewritten as $4^y \equiv 147 \times (4^{-10})^x \pmod{179}$.

Baby-step giant step example (continued)



We seek $x, y \in \{0, 1, \dots, 9\}$ with $4^y \equiv 147(4^{-10})^x \pmod{179}$.

We start by finding the residues of $4^y \pmod{179}$ for $0 \leq y \leq 9$:

$4^0 = 1, 4^1 = 4, 4^2 = 16, 4^3 = 64, 4^4 = 256 \equiv 77, 4^5 \equiv 129, 4^6 \equiv 158, 4^7 \equiv 95, 4^8 \equiv 22, 4^9 \equiv 88$.

As we compute these we sort them into increasing order, to make searching easier.

4^y	1	4	16	22	64	77	88	95	129	158
y	0	1	2	8	3	4	9	7	5	6

Of course if we had encountered 147 as one of the values of 4^y we would have stopped. (This would happen if $x = 0$.)

Now we compute $147(4^{-10})^x$ for $x = 1, 2$, etc., until we find one that appears in the table above.

Baby-step giant step example (concluded)



In fact $4^{-10} \equiv 149 \pmod{179}$.

Starting with 147, we repeatedly multiply by 149 and reduce mod 179, thus generating successive values of 147×149^x (reduced mod 179) for $x = 0, 1, 2, 3$, etc.:

$(x = 1)$	$147 \times 149 \equiv 65,$
$(x = 2)$	$65 \times 149 \equiv 19,$
$(x = 3)$	$19 \times 149 \equiv 146,$
$(x = 4)$	$146 \times 149 \equiv 95.$

Since 95 appears in our previously constructed list, we are finished.

We have found that $147 \times (4^{-10})^4 \equiv 95 \equiv 4^7 \pmod{179}$, and so $147 \equiv 4^{47} \pmod{179}$.

Pohlig-Hellman Algorithm



Suppose that we want to solve $b^i \equiv a \pmod{p}$. If we can factorize $k = \text{ord}_p(b)$ then we can simplify the problem.

Example: Solve $7^i \equiv 12 \pmod{41}$, given that $\text{ord}_{41}(7) = 40$.

Note that i is not uniquely determined; it is only determined modulo 40. Observe that $40 = 8 \times 5$.

Observe that 7^5 has order 8 and 7^8 has order 5 (mod 41).

Now $7^i \equiv 12$ gives $(7^8)^i \equiv 12^8$ and $(7^5)^i \equiv 12^5$.

Now $(7^8)^i \equiv 12^8$ determines i modulo 5 (since $\text{ord}_{41}(7^8) = 5$), and $(7^5)^i \equiv 12^5$ determines i modulo 8 (since $\text{ord}_{41}(7^5) = 8$).

Together these determine i modulo 40, by the Chinese Remainder Theorem.

Pohlig-Hellman example (continued)



We are solving $7^i \equiv 12 \pmod{41}$.

It is easily checked that $7^5 \equiv 38$ and $12^5 \equiv 3$.

So we want $38^i \equiv 3 \pmod{41}$.

Since $\text{ord}_{41}(38)$ is only 8, this can be solved quickly.

We find that $38^2 \equiv 9$, $38^3 \equiv 14$, $38^4 \equiv 40$, $38^5 \equiv 3$.

So $i \equiv 5 \pmod{8}$.

Similarly, since $7^8 \equiv 37$ and $12^8 \equiv 18$, we require $37^i \equiv 18$.

Since $\text{ord}_{41}(37)$ is only 5, this can be solved quickly.

We find that $37^2 \equiv 16$, $37^3 \equiv 18$. So $i \equiv 3 \pmod{5}$.

$i \equiv 5 \pmod{8}$ and $i \equiv 3 \pmod{5}$ together give $i \equiv 13 \pmod{40}$.

Another Pohlig-Hellman example



Example: Solve $11^i \equiv 25428 \pmod{54001}$, given that $54001 = p$ is prime and $\text{ord}_p(11) = p - 1 = 54000$.

Factorize $p - 1$: we find that $54000 = 2^4 \times 3^3 \times 5^3$.

We will find the residues of $i \pmod{2^4}$, $\pmod{3^3}$ and $\pmod{5^3}$, and then use the CRT to get i modulo 54000.

To help find the residue of $i \pmod{5^3}$ we first find its residue mod 5 and then find its residue mod 5^2 .

$54000 = 10800 \times 5$; so $\text{ord}_p(11^{10800}) = 5$.

We compute $(11^{10800})^0 \equiv 1$, $(11^{10800})^1 \equiv 18177$, $(11^{10800})^2 \equiv 25211$, $(11^{10800})^3 \equiv 7861$, $(11^{10800})^4 \equiv 2751$.

Now $11^i \equiv 25428$ gives $(11^{10800})^i \equiv 25428^{10800} \equiv 7861$.

So $i \equiv 3 \pmod{5}$.

Second P-H example (page 2)



We are solving $11^i \equiv 25428 \pmod{54001}$.

We have found that $i \equiv 3 \pmod{5}$. So $i - 3 = 5j$ for some j .

Now $11^{5j} \equiv 11^{i-3} \equiv 25428 \times 11^{-3} \equiv 22861$.

So $(11^{10800})^j \equiv (11^{5j})^{2160} \equiv 22861^{2160} \equiv 25211$.

We found previously that $25211 \equiv (11^{10800})^2$; so $j \equiv 2 \pmod{5}$.

Thus $i - 3 = 5j = 5(5\ell + 2)$ for some ℓ . That is, $i - 13 = 25\ell$.

Second P-H example (page 3)



We are solving $11^i \equiv 25428 \pmod{54001}$.

We have found that $i - 13 = 25\ell$ for some ℓ .

Now $11^{25\ell} \equiv 11^{i-13} \equiv 25428 \times 11^{-13} \equiv 18066$.

So $(11^{10800})^\ell \equiv (11^{25\ell})^{432} \equiv 18066^{432} \equiv 25211$.

We found previously that $25211 \equiv (11^{10800})^2$; so $\ell \equiv 2 \pmod{5}$.

Thus $i - 13 = 25\ell = 25(5\ell' + 2)$ for some ℓ' .

That is, $i - 63 = 125\ell'$.

So we have found that $i \equiv 63 \pmod{125}$ ($= 5^3$).

Second P-H example (page 4)



We treat the other prime factors of 54000 (namely 3 and 2) similarly.

Since $54000 = 18000 \times 3$ we see that $\text{ord}_p(11^{18000}) = 3$.

We compute $(11^{18000})^0 \equiv 1$, $(11^{18000})^1 \equiv 39940$,
 $(11^{18000})^2 \equiv 14060$.

Now $11^i \equiv 25428$ gives $(11^{18000})^i \equiv 25428^{18000} \equiv 14060$.

So $i \equiv 2 \pmod{3}$, giving $i - 2 = 3m$ for some m ,

Now $11^{3m} \equiv 11^{i-2} \equiv 25428 \times 11^{-2} \equiv 35467$.

So $(11^{18000})^m \equiv (11^{3m})^{6000} \equiv 35467^{6000} \equiv 39940$.

So $m \equiv 1 \pmod{3}$, and $i - 2 = 3(3n + 1)$ for some n .

Second P-H example (page 5)



We have $i - 5 = 9n$ for some n .

Now $11^{9n} \equiv 11^{i-5} \equiv 25428 \times 11^{-5} \equiv 26520$.

So $(11^{18000})^n \equiv (11^{9n})^{2000} \equiv 26520^{2000} \equiv 14060$,
giving $n \equiv 2 \pmod{3}$.

Thus $i - 5 = 9n = 9(3n' + 2)$ for some n' , and $i \equiv 23 \pmod{27}$.

The remaining prime factor of $p - 1$ is 2.

We know that $\text{ord}_p(11^{27000}) = 2$.

We have that $(11^{27000})^0 \equiv 1$ and $(11^{27000})^1 \equiv 54000$.

$11^i \equiv 25428$ gives $(11^{27000})^i \equiv 25428^{27000} \equiv 54000$.

So $i \equiv 1 \pmod{2}$.

Second P-H example (page 6)



We have $i - 1 = 2r$ for some r

So $11^i \equiv 25428$ gives $11^{2r} \equiv 25428 \times 11^{-1} \equiv 12130$.

Hence $(11^{27000})^r \equiv (11^{2r})^{13500} \equiv 12130^{13500} \equiv 54000$,
and so $r \equiv 1 \pmod{2}$.

Thus $i - 1 = 2(2s + 1)$ for some s , giving $i - 3 = 4s$.

$11^{4s} \equiv 11^{i-3} \equiv 25428 \times 11^{-3} \equiv 22861$.

$(11^{27000})^s \equiv (11^{4s})^{6750} \equiv 22861^{6750} \equiv 54000$. So $s \equiv 1 \pmod{2}$.

This gives $i - 3 = 4(2t + 1)$ for some t ; that is, $i - 7 = 8t$.

$11^{8t} \equiv 11^{i-7} \equiv 25428 \times 11^{-7} \equiv 32352$.

$(11^{27000})^t \equiv (11^{8t})^{3375} \equiv 32352^{3375} \equiv 54000$.

So $t \equiv 1 \pmod{2}$, and $i - 7 = 8(2u + 1)$ for some u .

So $i \equiv 15 \pmod{16}$.

The end of this example (finally)



All that remains is to solve

$$i \equiv 63 \pmod{125},$$

$$i \equiv 23 \pmod{27},$$

$$i \equiv 15 \pmod{16}.$$

It turns out that the solution is $i \equiv 14063 \pmod{54000}$.

Thus we have found that $11^{14063} \equiv 25428 \pmod{54001}$.