

Math 104B, Number Theory, Winter 2003.

Lecture 1. This quarter I plan to skip the applications of number theory to cryptography in order to understand the theory of quadratic forms. For example, how do you determine whether the number 261 is a sum of two squares? The answer is that you write the prime factorization $261 = 3^2 \cdot 29$, you see that $29 \equiv 1 \pmod{4}$, and so 261 is a sum of two squares! In general a prime is a sum of two squares if and only if it is congruent to 1 modulo 4. If $n = 2^{a_0} p_1^{a_1} \cdots p_j^{a_j} q_1^{b_1} \cdots q_k^{b_k}$ where p_1, \dots, p_j are distinct primes congruent to 3 modulo 4 and q_1, \dots, q_k are distinct primes congruent to 1 modulo 4, then n is a sum of two squares if and only if a_0, a_1, \dots, a_j are even!

We start today by introducing the concept of order, see **Definition 7.1.1**. If $m > 0$ and $(a, m) = 1$, then the order of a modulo n (denoted $\text{ord}_m(a)$) is the smallest positive k with $a^k \equiv 1 \pmod{m}$.

Examples. Let's compute the order of elements modulo 9. Since $\phi(9) = 6$, by Euler's Theorem, if $(a, 9) = 1$ then $a^6 \equiv 1 \pmod{9}$. Hence the maximum possible order of a modulo 9 is 6.

k	1	2	3	4	5	6
$2^k \pmod{9}$	2	4	8	7	5	1
$4^k \pmod{9}$	4	7	1			
$5^k \equiv 2^{5k} \pmod{9}$	5	7	8	4	2	1
$7^k \equiv 2^{4k} \pmod{9}$	7	4	1			
$8^k \equiv 2^{3k} \pmod{9}$	8	1				

We can compute $a^k \pmod{9}$ by writing $a = 2^b$, so $a^k \equiv 2^{bk}$, but since $2^6 \equiv 1 \pmod{9}$, if $bk \equiv c \pmod{6}$ then $2^{bk} \equiv 2^c \pmod{9}$. This is made precise in the second Corollary

below.

k	1	2	3	4	5	6
$5k \pmod{6}$	5	4	3	2	1	0
$4k \pmod{6}$	4	2	0			
$3k \pmod{6}$	3	0				

To summarize, there are two elements of order 6 and these are 2 and $2^5 \equiv 5$. An element which has order $\phi(m)$ modulo m is called a *primitive root* modulo m . WE see that 2 and 5 are primitive roots modulo 9.

There are two elements of order 3 and these are $2^2 \equiv 4$ and $2^4 \equiv 7$, there is one element of order 2 which is $2^3 \equiv 8 \equiv -1$, and one element of order 1 which is 1.

Here are some results which are illustrated by the previous example.

Proposition 1. See Prop. 7.1.3. If $a^k \equiv 1 \pmod{m}$ then $\text{ord}_m(a) | k$, in particular by Euler's Theorem, $\text{ord}_m(a) | \phi(m)$.

Corollary. See Cor. 7.1.4. If $(a, m) = 1$ then $a^i \equiv a^j \pmod{m} \Leftrightarrow i \equiv j \pmod{\text{ord}_m(a)}$.

Corollary. See Cor. 7.1.6. The elements $a, a^2, \dots, a^{\text{ord}_m(a)}$ are distinct modulo m .

Proposition 2. See Lem. 7.1.8. If $(a, m) = 1$, then

$$\text{ord}_n(a^k) = \frac{\text{ord}_n(a)}{(k, \text{ord}_n(a))}.$$

Proposition 3. See Cor. 7.2.9. The number of elements of order d modulo m in the set $\{a, a^2, \dots, a^{\text{ord}_m(a)}\}$ is $\phi(d)$ if $d | \text{ord}_m(a)$ and 0 otherwise. In particular, if there exists a primitive root modulo m then the number of invertible elements of order d is $\phi(d)$ if $d | \phi(m)$ and 0 otherwise.

Theorem. See Props. 7.1.13 and 7.1.14, and Ths. 7.2.8 and 7.2.10. There exists a primitive root modulo m if and only if m is of the form $2, 4, p^k$, or $2p^k$ where p is an odd prime.

Following Kumanduri-Romero, we proved Proposition 1 and the two Corollaries.

Example. Calculate the order of 3 and 9 modulo 23. How many elements of each order modulo 23 are there? Find a primitive root modulo modulo 23.

Solution. Since $\phi(23) = 22$, the order is either 2, 11 or 22. Now using successive squaring, $3^2 = 9$, $3^4 = 81 \equiv 12$, $3^8 \equiv 144 \equiv 6$, so $3^{11} \equiv 6 \cdot 9 \cdot 3 \equiv 1$. Hence $\text{ord}_{23}(3) = 11$. Since $9 = 3^2$, its order is

$$\frac{11}{(11, 2)} = 11.$$

By the Theorem, we know that there is a primitive root modulo 23. Hence by Proposition 3, there are 10 elements of order 22, there are 10 elements of order 11, there is 1 element of order 2, and 1 of order 1. This accounts for all the 22 invertible elements. Let's compute the powers of 2.

k	1	2	3	4	5	6
$2^k \pmod{23}$	2	4	8	16	9	18
k	7	8	9	10	11	
$2^k \pmod{23}$	13	3	6	12	1	

We get the 10 elements of order 11. We take a number other than these and the numbers ± 1 . This leaves us with the elements of order 22. For example, 5 is a primitive root.