Public Key Cryptosystems

1 Primitive Roots

Given a prime p, an integer q is said to be a *primitive root* mod p if the numbers

$$q^1, q^2, q^3, \ldots, q^{p-1}$$

are all distinct mod p. For instance 2 is a primitive root mod 13, since the successive 12 powers of 2 mod 13 are

s	1	2	3	4	5	6	7	8	9	10	11	12
2^s	2	4	8	3	6	12	11	9	5	10	7	1

The knowledge of a primitive root enables us to solve several congruence problems with the greatest of ease. For instance suppose we wish to find the solution of the congruence

$$11x \equiv 9 \mod 13 \tag{1.1}$$

Looking at the above table we see that

$$11 \equiv 2^7 \text{ and } 9 \equiv 2^8 \mod 13$$

this given, setting $x = 2^y$, equation (1.1) can be rewritten in the form

$$2^{7+y} \equiv 2^8 \mod 13 \tag{1.2}$$

Note now that by Fermat's theorem we have $2^{12} \equiv 1 \bmod 13$, this implies that for any a we have

$$2^a 2^{12-a} \equiv 2^{a+12-a} \equiv 2^{12} \equiv 1 \mod 13$$

Using this with $a = 7$ in 2 gives that

$$x \equiv 2^y \equiv 2^5 2^8 \equiv 2^{5+8} \equiv 2^1 \equiv 2 \mod 13$$

The calculation we have carried out in this example should remind us precisely of what we usually do when solving equations such as (1.1) using a logarithm table. Indeed, the table above gives us precisely the "logarithms" of the different integers mod 13 in the "base" 2. The computations are entirely analogous, with the only difference being the fact that calculations in the exponents need to be done "mod 12" in this case, and "mod $p-1$" for the case of a general prime p.

Let us look at another example. For $p = 29$ we note that the primitive roots are

$$2, 8, 3, 19, 18, 14, 27, 21, 26, 10, 11, \text{ and } 15.$$

Choosing again 2 we can easily construct the following table

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2^s	2	4	8	16	3	6	12	24	19	9	18	7	14	28

s	15	16	17	18	19	20	21	22	23	24	25	26	27	28
2^s	27	25	21	13	26	23	17	5	10	20	11	22	15	1

Once we notice that 2 is a primitive root mod 29, the remaining primitive roots may all be read off of the table above. If a is a primitive root mod p, then so will all powers a^s mod p where s is relatively prime to $p-1$. In particular, since 2 is a primitive root mod 29 then

$$2^1, 2^3, 2^5, 2^9, 2^{11}, 2^{13}, 2^{15}, 2^{17}, 2^{19}, 2^{23}, 2^{25}, 2^{27} \mod 29$$

will all be primitive roots.

Suppose then that we seek for the solution of the congruence

$$27^x \equiv 2 \mod 29 \tag{1.3}$$

Using the above table we can rewrite this equation in the form

$$2^{15\,x} \equiv 2^1 \mod 29 \tag{1.4}$$

Or better

$$2^{15\,x-1} \equiv 1 \mod 29 \tag{1.5}$$

Since 2 is a primitive root, this can only hold if

$$15\,x - 1 \equiv 0 \mod 28$$

Using the Euclidean algorithm we find

$$1 = 7 \times 28 - 13 \times 15$$

and this gives

$$-13 \times 15 \equiv 1 \mod 28$$

so then the solution of (1.3) is

$$x \equiv -13 \equiv 15 \mod 28$$

Equation (1.3) is an instance of what is usually referred to as the "*discrete logarithm problem*". Now it develops that without the previous construction of the "*logarithm table*" such equations are difficult to solve. Given a very large prime p, the assembly of the table for any give primitive root is out of the question.

For any prime p we can always find a primitive root. There is a beautiful result in this respect which can be stated as follows.

Theorem 1.1 *For a given prime p there are exactly $\phi(p-1)$ primitive roots.*

The proof of this theorem may be found in the "Cyclotomic Polynomials and Primitive roots" handout.

However, we should note that it is easy to see that if there is a single primitive root q then there will be exactly $\phi(p-1)$ all together. The reason for this is that all the other primitive roots are the integers Q such that the equation

$$Q^x \equiv q \pmod p$$

can be solved for x. Now, since every such Q can be written in the form $Q = q^y$ for some y, we deduce that each Q corresponds to a pair (x, y) such that $xy \equiv 1 \pmod{p-1}$. Now these y's are precisely the numbers less than $p-1$ that are relatively prime to $p-1$.

2 Diffie-Hellman Public Key Exchange

We are now in posession of a mechanism that allows a group of people to use one method of encryption for everyone while at the same time insures that any two people can have a private conversation. Since the method of encrpytion is fixed, in order for two people to speak privately, they must be able to agree upon a common key that only they could possibly know. Here is how it works.

Our collection of people $p_1, p_2, \ldots, p_6$ first agree on a modulus, p, in which they do their computations. For example, let's say that they agree on the number 37.

They also agree on a common base, a, which they will raise to some powers later on. In this case, they choose base 17. This base must be a primitive root of p. In other words, every integer from 1 to $p-1$ must be represented by some power of a.

Each person then secretly selects a number from 1 to $p-1$. In this case, p_3 selects 10 and p_6 selects 9. Now, p_3 and p_6 may create their own common key, known by nobody else, without compromising their own secret number. To do this, p_3 publicly sends p_6 the value

$$17^{10} \mod 37 = 28$$

and tells p_6 to raise it to his secret number. Now, p_6 has the number

$$28^{9} \mod 37 = 36$$

In return, p_6 sends p_3 the value

$$17^{9} \mod 37 = 6$$

and p_3 raises that to his secret number to get

$$6^{10} \mod 37 = 36$$

So p_3 and p_6 both have the number 36, known to nobody else and neither person gave away their private key. This common key, 36, can now be used as the key for any secret communication between p_3 and p_6. For example, they may decide to encrypt with Vigenere, using the digits of the key as shift values. Or they may use the ElGamal Public Key System.

3 ElGamal Public Key System

Using the "fact" that the logarithm problem is (probably) difficult, one can set up the following public Key system.

1. First, choose a global prime p (larger than 150 digits), such that $p-1$ has at least one "large" factor, and let a be a primitive root for p.

2. Each participant i chooses (at random) a secret number S_i in the interval $\{1, \ldots, p-1\}$, and sets
$$\beta_i := a^{S_i} \mod p.$$

3. The values p, a, and β_i are all made public.

To send a message X to **Bob** using his public key β, **Alice** chooses at random a secret number S_A in the interval $\{1, \ldots, p-1\}$, and sends the pair

$$(Y, Z), \qquad \text{where} \qquad Y := a^{S_A} \pmod{p}, \quad \text{and} \quad Z := X\,\beta^{S_A} \pmod{p}$$

Bob can then get X back using his secret exponent S_B:

$$X \equiv Z\,(Y^{S_B})^{-1} \pmod{p}.$$

In this, we can consider that Y is used to "encode" S_A.

Exercises:

1. Prove that 2 is not a primitive root mod 17.
2. Prove that 3 is a primitive root mod 17 and then find all the primitive roots mod 17.
3. Construct a logarithm table mod 29 using the primitive root 3.
4. Use the tables from the previous exercise or in the text above to solve the following congruences mod 29.

   (a) $x \equiv (12)(13)$
   (b) $x \equiv (21)(25)$
   (c) $3x \equiv 7$
   (d) $17x \equiv 23$
   (e) $8x \equiv 1$
   (f) $x \equiv 15^{10}$
   (g) $x \equiv 13^{23}$
   (h) $x^2 \equiv 16$
   (i) $x^2 \equiv 18$
   (j) $x^2 \equiv 7$
   (k) $x^3 \equiv 18$
   (l) $x^4 \equiv 22$

5. Six individuals $P_1, P_2, \ldots, P_6$ establish a public key system based on the modulus 37 and primitve root 18. Suppose that the published keys are

   $$k_1 = 6 \quad k_2 = 5 \quad k_3 = 12 \quad k_4 = 7 \quad k_5 = 28 \quad k_6 = 4.$$

   To eavesdrop on a communication between P_2 and P_6 you should have their common key $k_{2,6}$. Calculate it. For your convenience we give below the table of powers of 2 modulo 37.

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^i	2	4	8	16	32	27	17	34	31	25	13	26	15	30	23	9	18	36

19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
35	33	29	21	5	10	20	3	6	12	24	11	22	7	14	28	19	1

6. Alice and Bob agree to communicate using the primitive root 15 and the modulus 37. If Alice choses a secret key of 5 and Bob choses a secret key of 11, then find Alice and Bob's common key.
7. Suppose that in an ElGamal system we have $p = 2579$ and $a = 2$. If Bob's secret exponent is $S_B = 765$ and Alice's secret exponent is $S_A = 23$, compute Bob's public key β, and encode Alice's message $X = 1299$.