Group Example

Yehuda Lindell

January 4, 2012

I will present an example of a prime-order group that we use for DDH. I will first give the general definition of the group and then a concrete example with small numbers.

General definition. Let p be a prime such that $(p-1)/2$ is also a prime (equivalently, $p = 2q+1$ and both p and q are prime). Let g be a generator of the subgroup of $\mathbb{Z}_p^*$ of order q. As we will see, such a subgroup can be taken to be all of the values that have a square root modulo p. Note that $\mathbb{Z}_p^*$ itself has $p-1$ elements and so does not have a prime order. For this reason, we take a subgroup of order q. (Note also that $\mathbb{Z}_p$, which includes the numbers from 0 to $p-1$ and so includes 0 is not a multiplicative group. This is due to the fact that 0 has no inverse.)

Example. Let $p = 11$ and $q = 5$. First consider the group $\mathbb{Z}_{11}^*$. This is a multiplicative group over the number $1, 2, \ldots, 10$. It is not hard to see that all values have an inverse, as can be seen in this table (recall, the inverse of a number a is the number b so that $a \cdot b$ equals 1 modulo $p = 11$):

Number:	1	2	3	4	5	6	7	8	9	10
Inverse:	1	6	4	3	9	2	8	7	5	10

Note that 5 is the inverse of 9 because $5 \cdot 9 = 45$ which when divided by 11 gives remainder 1.

Let us now find a generator of $\mathbb{Z}_{11}^*$. We will try one by one to see what happens:

Series based on 2:	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9
Values received:	1	2	4	8	5	10	9	7	3	6

We got lucky the first time. The number 2 is a generator! Let's try 3:

Series based on 3:	3^0	3^1	3^2	3^3	3^4	3^5	3^6	3^7	3^8	3^9
Values received:	1	3	9	5	4	1	3	9	5	4

and so 3 is not a generator of the entire group. Rather, it generates a subgroup with numbers $1, 3, 4, 5, 9$. That is, 3 generates a *subgroup* of order 5 (which is prime!). Note: the fact that this is a subgroup means that if you multiply any of the numbers in the subgroup (modulo 11) the result is one of the numbers. For example, $3 \cdot 5$ equals 4, and $3 \cdot 9 = 5$.

Now, let's see what happens with 10:

Series based on 10:	10^0	10^1	10^2	10^3	10^4	10^5	10^6	10^7	10^8	10^9
Values received:	1	10	1	10	1	10	1	10	1	10

which holds because $10^2 = 100$ and when divided by 11 this has remainder 1. In general, for every divisor of $p-1$ there is a subgroup of that size (here the divisors are 5 and 2, and in general when $p = 2q+1$ they are q and 2).

We want to work in a subgroup of order q. How do we find such a subgroup? First, we can just try and find an element of this order (this isn't too hard). Also, it turns out that these are all the values with square roots modulo p. Let's see:

Number:	1	2	3	4	5	6	7	8	9	10
Square:	1	4	9	5	3	3	5	9	4	1

This means that the number that have square roots are $1, 3, 4, 5, 9$ (any number that is a square, has a square root), which is exactly the same subgroup as above.

Using our general notation, we have that the group $\mathbb{G}$ equals the numbers $1, 3, 4, 5, 9$ together with the operation which "multiplication modulo 11 (any group is defined by values and an operation), the generator is $g = 3$, and the order is $q = 5$. (Note that any number apart from 1 is a generator in a prime-order group. However, it is important that we refer to one specific one, like $g = 3$ here.)

Choosing a random value in the subgroup. There are two possibilities in the above example:

1. Take a generator of the subgroup, e.g., 3 and then compute 3^x for a random x between 1 and 10. Since every square can be obtained with exactly two possible x's (e.g., 9 is obtained by 3^2 and 3^8), each value of $1, 3, 4, 5, 9$ has exactly the same probability of being chosen. This is a general method that works for *any* group and *any* subgroup.

2. In this specific example, you can also choose a random value between 1 and 10 and square it modulo 11. This has the same effect and can be used for the specific subgroup of order q where $q = 2p + 1$.[1]

[1]The advantage of this method is that you can map an arbitrary string into the subgroup and back. In order to see this, note that the squares are arranged so that they appear separately in each half (first $1, 4, 9, 5, 3$ and then $3, 5, 9, 4, 1$). The reason for this is that $(-1)^2 = 1$ and so for any value a it holds that $a^2 = (-a)^2$. Thus, $3^2 = (-3)^2 = 9 \bmod 11$, but $-3 = 8$ when working modulo 11. Using this, we can take any binary string α of an appropriate length and look at it as a number between 1 and $(p-1)/2 = q$. Then, we map the string α into the group by computing $a = \alpha^2 \bmod p$. Furthermore, given any value a in the subgroup, we can get α back by computing $\alpha = \sqrt{a} \bmod p$ (this can be efficiently done modulo a prime). (Mapping into the subgroup can also be carried out by computing g^α according to the previous method of getting a value in the subgroup. However, due to the difficulty of computing the discrete log in large groups, you cannot map back.)