Semester 1 **Exercises and Solutions for Week 12** 2004

Diffie–Hellman and Discrete Logarithms

An El Gamal cryptosystem is based on the difficulty of the Diffie–Hellman problem: Given a prime p, a primitive element a of $(\mathbb{Z}/p\mathbb{Z})^* = \{c \in Z/pZ : c \neq 0\}$, and elements $c_1 = a^x$ and $c_2 = a^y$, find the element a^{xy} in $(\mathbb{Z}/p\mathbb{Z})^*$.

1. Recall the discrete logarithm problem: Given a prime p, a primitive element a of $(\mathbb{Z}/p\mathbb{Z})^*$, and an element c of $(\mathbb{Z}/p\mathbb{Z})^*$, find an integer x such that $c = a^x$. Explain how a general solution to the discrete logarithm problem for p and a implies a solution to the Diffie–Hellman problem.

Solution Suppose that the discrete logarithm problem has an efficient solution. Then, given a primitive element a of $\mathbb{F}_p$, for every a^x and a^y we could solve for $x = \log_a(a^x)$ and for $y = \log_a(a^y)$. It follows that we could then produce the value a^{xy}, which solves the Diffie-Hellman problem.

2. Fermat's little theorem tells us that $a^{p-1} = 1$ for all a in $(\mathbb{Z}/p\mathbb{Z})^*$. Recall that a primitive element a has the property that $\mathbb{Z}/(p-1)\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})^*$ given by $x \mapsto a^x$ is a bijection.

a. Show that a is primitive if and only if $a^x = 1$ only when $p - 1$ divides x.

b. Let p be prime $2^{32} + 15$. Show that $a = 3$ is a primitive element of $(\mathbb{Z}/p\mathbb{Z})^*$. Use the `Magma` function `Log` to compute discrete logarithms of elements of `FiniteField(p)` with respect to a.

c. Let p be the prime $2^{32}+61$. Show that the element $a = 2$ is a primitive element for $(\mathbb{Z}/p\mathbb{Z})^*$. Use the `Magma` function `Log` to compute discrete logarithms of elements of `FiniteField(p)` with respect to a.

Solution The statement of the definition of primitive is a formal statement equivalent to that which follows. An element a of $\mathbb{Z}/p\mathbb{Z}$ is primitive if and only if

$$1, a, a^2, \ldots, a^{p-2}$$

are all distinct, and therefore enumerate all nonzero elements of $\mathbb{Z}/p\mathbb{Z}$.

a. Fermat's little theorem tells us that the next value, a^{p-1} in this list is 1, and therefore $a^x = 1$ for all $x = r(p-1)$, and indeed, we have run out of nonzero elements so must have a repeat at this point.

Conversely for any nonzero element a there must be some value t such that $a^t = 1$, hence $a^{rt} = 1$ for all r. We may assume that t divides $p-1$, since if $t' = \mathrm{GCD}(t, p-1)$ then there exist r and s such that $t' = rt + s(p-1)$, so

$$1 = a^{rt}a^{s(p-1)} = a^{rt+s(p-1)} = a^{t'},$$

and we can replace t by t'. Therefore the maximum length of a cycle $1, a, a^2, \ldots, a^{t-1}$ divides $p-1$ and is equal l to $p-1$ exactly when a is primitive.

b. For $p = 2^{32} + 15$, the factorization of $p-1$ is $2 \cdot 3^2 \cdot 5 \cdot 131 \cdot 364289$. We need to check that 3^x is not 1 mod p for any divisor of $p-1$.

```
> p := 2^32+15;
> Modexp(3,(p-1) div 2,p);
4294967310
> Modexp(3,(p-1) div 3,p);
2086193154
> Modexp(3,(p-1) div 5,p);
239247313
> Modexp(3,(p-1) div 131,p);
1859000016
> Modexp(3,(p-1) div 364289,p);
1338913740
```

How does this prove that 3 is a primitive element?

By producing random elements in $\mathbb{F}_p$ and computing discrete logarithms with respect to a, we find that the time to compute discrete logarithms in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is trivial.

```
> FF := FiniteField(p);
> for i in [1..4] do
>     time x := Log(FF!3,Random(FF));
> end for;
Time: 0.010
Time: 0.000
Time: 0.000
Time: 0.000
```

c. For $p = 2^{32} + 61$, the factorization of $p-1$ is $2^2 \cdot 1073741839$. We repeat the same test as in the previous part.

```
> p := 2^32+61;
> Modexp(2,(p-1) div 2,p);
4294967356
> Modexp(2,(p-1) div 1073741839,p);
16
```

The shows that 2 is a primitive element. Next we find that, for this prime p, that the time to compute discrete logarithms in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is nontrivial.

```
> FF := FiniteField(p);
> for i in [1..4] do
```

```
>     time x := Log(FF!2,Random(FF));
> end for;
Time: 0.510
Time: 0.460
Time: 0.460
Time: 0.650
```

3. Compare the times to compute discrete logarithms in the previous exercise. Now factor $p-1$ for each p. What difference do you note? Explain the timings in terms of the Chinese remainder theorem for $\mathbb{Z}/(p-1)\mathbb{Z}$.

Solution The nontrivial time for the discrete logarithm is due to the large prime divisor of $p-1$. The amount of time required to compute a discrete logarithm in $\mathbb{F}_p$ is dependent on the size of the largest prime divisor of $p-1$. The discrete logarithm can be computed independently for each prime divisor of $p-1$ — more correctly for prime power divisor — and the discrete logarithm can be recovered by the Chinese remainder theorem, as is the next example.

4. Let p be the prime $2^{131}+1883$ and verify the factorization

$$p-1 = 2\cdot 3\cdot 5\cdot 37\cdot 634466267339108669\cdot 3865430919824322067.$$

Let $a = 109$ and $c = 10144521312305511283199283124348697683 46$ and set

$$n_5 = (p-1) \text{ div } 634466267339108669$$
$$n_6 = (p-1) \text{ div } 3865430919824322067.$$

Then verify that $c^{n_5} = a^{129n_5}$ and $c^{n_6} = a^{127n_6}$. Find similar relations for

$$n_1 = (p-1) \text{ div } 2 \quad n_3 = (p-1) \text{ div } 5,$$
$$n_2 = (p-1) \text{ div } 3 \quad n_4 = (p-1) \text{ div } 37.$$

and use this information to find the discrete logarithm of c with respect to a.

Solution We set up the problem in `Magma` in the following way.

```
> p := 2^131+1883;
> fac := Factorization(p-1);
> TrialDivision(p-1);
[ <2, 1>, <3, 1>, <5, 1>, <37, 1> ]
[ 24524855273581150519882854589676988 23 ]
> Factorization(24524855273581150519882854589676988 23);
[ <634466267339108669, 1>, <3865430919824322067, 1> ]
> primes := [ f[1] : f in Factorization(p-1) ];
> p1, p2, p3, p4, p5, p6 := Explode(primes);
> exponents := [ (p-1) div r : r in primes ];
> n1, n2, n3, n4, n5, n6 := Explode(exponents);
> FF := FiniteField(p);
> a := FF!109;
> c := FF!10144521312305511283199283124348697683 46;
```

where the command `Explode` outputs the elements of the sequence so that we can assign them to variables n_1, n_2, n_3, n_4, n_5, and n_6.

Raising both generator a and its power c to the large exponents n_1, n_2, n_3, and n_4 reduces the solution to the discrete logarithm to one modulo $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, and $p_4 = 37$, which can be easily solved by enumerating all possibilities.

```
> Index({@ a^(n1*i) : i in [1..2] @}, c^n1);
1
> Index({@ a^(n2*i) : i in [1..3] @}, c^n2);
2
> Index({@ a^(n3*i) : i in [1..5] @}, c^n3);
4
> Index({@ a^(n4*i) : i in [1..37] @}, c^n4);
29
> CRT([1,2,4,29],[2,3,5,37]);
29
```

For the larger primes

$$p_5 = 634466267339108669 \text{ and } p_6 = 3865430919824322067,$$

we verify the given discrete logarithms.

```
> a5 := a^n5;
> c5 := c^n5;
> a5^129;
1106532280219457618983939634726858708298
> c5;
1106532280219457618983939634726858708298
> a6 := a^n6;
> c6 := c^n6;
> a6^127;
809579285918008980133272648385832028198
> c6;
809579285918008980133272648385832028198
```

The discrete logarithm x can be recovered from the discrete logarithms $x_i = \log_{a_i}(c_i)$ where $a_i = a^{n_i}$ and $c_i = c^{n_i}$ by using the function `CRT` to find the Chinese remainder lifting.

```
> x := CRT([29,129,127],[2*3*5*37,p5,p6]);
> x;
107521720347655517565250443822403757 9
> a^x eq c;
true
```