THE UNIVERSITY OF SYDNEY
MATH3925 PUBLIC KEY CRYPTOGRAPHY

Semester 2 **Solutions for Assignment 2** 2004

This assignment will be due on Friday 24 September, should be submitted at 638 Carslaw by 5PM, and is worth 10% of the assessment for this course.

1. Let n be the integer 228618946967762521. Explain how 3-torsion elements in $\mathbb{Z}/n\mathbb{Z}^*$ can be used to factor n, and demonstrate this with $x = 902089523684315 23$.

Solution A three torsion element x satisfies a relation $x^3 - 1 = 0$, which can be written in factored form as $(x-1)(x^2+x+1) = 0$. Over a field such a relation implies that $x - 1 = 0$ or $x^2 + x + 1 = 0$, but in $\mathbb{Z}/n\mathbb{Z}$, where $n = pq$ any of the possible combinations of relations modulo p and modulo q can occur:

$x-1 \bmod p$	$x^2+x+1 \bmod p$	$x-1 \bmod q$	$x^2+x+1 \bmod q$
0	$*$	0	$*$
$*$	0	0	$*$
0	$*$	$*$	0
$*$	0	$*$	0

Note that there exist either 2 or 0 solutions to $x^2+x+1 \bmod p$, depending whether 3 divides $p-1$ or not. Provided one of $p-1$ and not $q-1$ is divisible by 3, there is a 2/3 chance that a random 3-torsion element x finds the factor $q = \mathrm{GCD}(x-1, n)$, and if both $p-1$ and $q-1$ are divisible by 3 then there is a 4/9 chance that $\mathrm{GCD}(x-1, n$ finds p or q. In this case we find

$$\mathrm{GCD}(x-1, n) = \mathrm{GCD}(x-1, n) = 933376471.$$

Note that unlike 3 (or 5, 7, etc.), the prime 2 always divides $p-1$ and $q-1$, which is why we give emphasis to finding 2-torsion.

2. **a.** Find the discrete logarithm x of 2 with respect to the base 3 in $\mathbb{F}_p^*$, where $p = 1234621183$. Use the Pollig-Hellman reduction, noting that $p - 1 = 2 \cdot 3 \cdot 83 \cdot 383 \cdot 6473$, and give the values you determine for $x \bmod 2, x \bmod 3$, etc.

b. Now determine the discrete logarithm $\log_3(2)$ in $\mathbb{F}_p^*$, where $p = 65537$, expressing the result in base 2.

Solution

a. The discrete logarithm $\log_2(3)$ in $\mathbb{F}_p$ is well-defined as an element of the additive group $\mathbb{Z}/(p-1)\mathbb{Z}$. It can be computed modulo each prime divisor r of $p-1$

by setting $m = (p-1)/r$ (using the `Magma` operator `div`), and computing $x = \log_{2^m}(3^m) \bmod r$.

x	r
0	2
0	3
56	83
215	383
5635	6473

Using the Chinese remainder theorem, we recover $k = 389634924$.

b. Since $p-1 = 2^{16}$, we solve iteratively for the 16-bits of the discrete logarithm, $x = 1101100000000000_2 = 55296$. Explicitly, we find that $3^{2^{15}} = -1$ so it generates $\mathbb{F}_p^*$, then $2^{2^{15}} = \cdots = 2^{2^5} = 1$, so the least significant 11 bits are all 0. Then $(2)^{2^4} = -1$, so the next bit is 1, $(3^{-2^{11}}2)^{2^3} = -1$, so again we have a bit 1, and $(3^{-2^{11}-2^{12}}2)^{2^2} = 1$, so the bit 0 follows, etc.

3. Verify that the ring $\mathbb{Z}[\tau]/(13)$, where $\tau^3 - \tau + 1 = 0$ is a field, that 61 divides the order of $\mathbb{Z}[\tau]/(13)^*$, and that $x = \tau + 6$ and $y = \tau + 10$ have exact order 61.

a. Partition $\mathbb{F}_{13^3}$ into disjoint sets

$$\begin{aligned} S_1 &= \{a + b\tau + c\tau^2 \in \mathbb{F}_{13^3} : 0 \le a \le 4\}, \\ S_2 &= \{a + b\tau + c\tau^2 \in \mathbb{F}_{13^3} : 5 \le a \le 8\}, \\ S_3 &= \{a + b\tau + c\tau^2 \in \mathbb{F}_{13^3} : 9 \le a\}, \end{aligned}$$

and use these to determine four cycles and tails in the Pollard ρ method beginning with an initial value of the form $x^n y^m$. Give both the elements $x^{n_i} y^{m_i}$ and the exponents (n_i, m_i) in the sequence. Use your cycles to determine the discrete logarithm $\log_x(y)$.

b. Find the complete set of relations between the elements

$$-1, \tau, 2, 3, \tau^2 + 1, \tau^2 + \tau + 1, -2\tau - 1, x, y$$

of $\mathbb{F}_{13^3}$, and demonstrate how to use these to determine $\log_x(y)$.

Solution Since $\tau^3 - \tau + 1 = 0$ has no solution τ in $\mathbb{F}_{13}$, it must be irreducible, hence $\mathbb{Z}[\tau]/(13)$ is a field. Since $13^3 - 1 = 36 \cdot 61$, there must be an element of order 61 in $\mathbb{Z}[\tau]/(13)^*$. The order of x and y can be verified computationally.

a. See Tutorial 6 for details of the Pollard ρ algorithm; a variety of sequences (x_i, n_i, m_i) are possible for the question. Note, however, that the length of the tails and the period can vary significantly, but most all result in the relation $xy^2 = 1$. From the order of the group we can write $y^2 = x^{61-1} = x^{60}$, so $y = x^{30}$. Therefore $\log_x(y) = 30$.

b. The full matrix of relations has a basis matrix of the form:

$$\begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 & -2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & -2 & 1 & 1 & -1 & 0 \\ 1 & 1 & 1 & -2 & 1 & 0 & 0 & -1 & 0 \\ 1 & -2 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 2 & 1 & 0 & 0 & 0 & 3 & 2 & 0 \end{bmatrix}.$$

Computing its echelon form, we find the basis matrix:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 18 & 0 & 22 \\ 0 & 1 & 0 & 0 & 0 & 0 & 30 & 0 & 43 \\ 0 & 0 & 1 & 0 & 0 & 0 & 15 & 0 & 59 \\ 0 & 0 & 0 & 1 & 0 & 0 & 24 & 0 & 9 \\ 0 & 0 & 0 & 0 & 1 & 0 & 21 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 19 & 0 & 56 \\ 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 44 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 61 \end{bmatrix}$$

This determines the same kernel group of relations, but now we can read off the relation $xy^2 = 1$ from the bottom right-hand corner. Using the relation $y^{61} = 1$, which we already knew but which appears at the lower right-hand entry, we compute $(xy^2)^{30}y = x^{30}y^{61} = y$, or $y = x^{30}$.