Technische Universität München (I7)
Dr. M. Luttenberger / M. Schlund

Winter term 2014/2015
Wednesday 21st January, 2015

Solution

Cryptography – Homework 5

Discussed on Tuesday, 9th December, 2014.

For questions regarding the exercises, please send an email to schlund@in.tum.de or just drop by at room 03.11.055

(∗) Starred exercises are optional and are usually not discussed during the tutorial (nevertheless they are fun—hopefully).

Exercise 5.1 Warm-up II

(a) $\mathbb{Z}_{54}^*$ is a cyclic group. What is its order? Determine a generator g of $\mathbb{Z}_{54}^*$ and solve $7^x \equiv 19 \bmod 54$ for x (i.e. compute the discrete logarithm of 19 to the base 7).

(b) Let $\pi = [23154] \in S_5$. Determine π^{842}.

(c) Compute the greatest common divisor d of 234, 762, and 139. Furthermore determine $r, s, t \in \mathbb{Z}$ such that $r \cdot 234 + s \cdot 762 + t \cdot 139 = d$.

(d) Solve for X: $X \equiv 2 \bmod 5 \wedge X \equiv 5 \bmod 11 \wedge X \equiv 1 \bmod 21$.

(e) We have seen that it is fairly easy to compute square roots modulo certain primes. Let $p = 47$. Solve for X: $X^2 \equiv 6 \bmod 47$ (*Hint*: $p \equiv 3 \bmod 4$ since p is a safe prime).

Solution:

(a) $|\mathbb{Z}_{54}^*| = \varphi(54) = \varphi(2 \cdot 3^3) = \varphi(2) \cdot \varphi(3^3) = 1 \cdot (3^3 - 3^2) = 18$. A possible generator is 5 because $5^9 \equiv_{54} 53 \neq 1$ and $5^6 \equiv_{54} 19 \neq 1$. A possible solution to $7^x \equiv_{54} 19$ is $x = 3$ (brute-force).

(b) $|S_5| = 5! = 120$, therefore $\pi^{842} = \pi^2 = [31245]$. Note that we can always reduce exponents modulo the order of the group we compute in!

(c) $\gcd(234, 762, 139) = \gcd(234, \gcd(762, 139)) = \gcd(234, 1) = 1$ (or shortcut: 139 is a prime therefore it must be 1)

(d) This is the CRT "backwards". We have $1 = 1 \cdot 11 - 2 \cdot 5$ and therefore the three equations reduce to two: $X = 2 \cdot 11 - 2 \cdot 5 \cdot 5 \bmod 55 \wedge X = 1 \bmod 21$. Which gives us $X = 27 \bmod 55 \wedge X = 1 \bmod 21$. By using the extended euclidean algorithm we get $1 = 21 \cdot 21 - 8 \cdot 55$ and thus the final solution is: $X = 27 \cdot 21 \cdot 21 - 1 \cdot 8 \cdot 55 \bmod 55 \cdot 21$ which is $X = 1072 \bmod 1155$. One can easily check that 1072 satisfies all three equations—so we have not made a mistake :).

(e) Modulo primes with $p \equiv 3 \bmod 4$ we can compute square-roots easily: $6^{\frac{p+1}{4}} = 6^{12} = 37 \bmod 47$. (Check: $37^2 = 6 \bmod 47$)

Exercise 5.2 Arithmetic Operations Modulo N

Please do the following calculations by hand :-)

(a) Compute 27^{-1} in $\mathbb{Z}_{100}^*$, and 25^{-1} in $\mathbb{Z}_{998}^*$ using the extended Euclidean algorithm.

(b) Compute $(4^{75} \bmod 18)$, $(4^{113} \bmod 14)$ and $(2^{5630} \bmod 29)$.

Solution:

(a) We compute 27^{-1} in $\mathbb{Z}_{100}^*$ by calculating $\gcd(100, 27)$:

a	b	Equation	Backsubstitution
27	100	$100 = 3 \cdot 27 + 19$	$1 = 10 \cdot 100 + (-37) \cdot 27$
19	27	$27 = 1 \cdot 19 + 8$	$1 = (-7) \cdot 27 + 10 \cdot 19$
8	19	$19 = 2 \cdot 8 + 3$	$1 = 3 \cdot 19 - 7 \cdot 8$
3	8	$8 = 2 \cdot 3 + 2$	$1 = (-1) \cdot 8 + 3 \cdot 3$
2	3	$3 = 1 \cdot 2 + 1$	$1 = 1 \cdot (3 - 1 \cdot 2) + 0 \cdot 2 = 1 \cdot 3 - 1 \cdot 2$
1	2	(Result 1)	$1 = 1 \cdot 1 + 0 \cdot 2$

We obtain $-37 \equiv 63 \pmod{100}$ as result and verify: $27 \cdot 63 = 1701 \equiv 1 \pmod{100}$. Similarly we can obtain $519 \cdot 25 \equiv 1 \pmod{998}$ for the second calculation.
In the exercise we introduced an easy iterative algorithm for exponentiation by squaring: Instead of computing the exponentiation recursively, one can use the binary represenation of the exponent for the computation. Assume we want to compute $a^b \bmod N$. Then we write $b = (b_1 \dots b_n)_2$ as the binary representation of b (msbf notation). We set $x := 1$ and $i = 1$ and process the bitstring from left to right:

(1) If $b_i = 1$ set $x := (x^2 \cdot a) \bmod N$.

(2) If $b_i = 0$ set $x := x^2 \bmod N$.

(3) If $i = n$, return x; else set $i := i + 1$ and goto 1.

We note that in total at most $2 \cdot n$ multiplications of n-bit integers are carried out by this method. For computing e.g. $(4^{75} \bmod 18)$, we write $75 = (1001011)_2$ and compute (computations modulo 18):

bits	$b_1 = 1$	$b_2 = 0$	$b_3 = 0$	$b_4 = 1$	$b_5 = 0$	$b_6 = 1$	$b_7 = 1$
Result (x):	4	$4^2 \equiv (-2)$	$(-2)^2 \equiv 4$	$(4)^2 \cdot 4 \equiv 10$	$10^2 \equiv 10$	$10^2 \cdot 4 \equiv 4$	$4^2 \cdot 4 \equiv 10$

Hence the result is $4^{75} \equiv 10 \pmod{18}$. Similarly one obtains $4^{113} \equiv 2 \pmod{14}$. For computing $(2^{5630} \bmod 29)$, since $gcd(2, 29) = 1$, we can compute modulo the order of $\mathbb{Z}_{29}^*$:
$(2^{5831} \bmod 29) \equiv (2^{5831 \bmod \phi(29)} \bmod 29) \equiv (2^{5630 \bmod 28} \bmod 29) \equiv (2^2 \bmod 29) = 4$.

Exercise 5.3 Applications of the CRT

The Chinese remainder theorem states that $\mathbb{Z}_{NM}^* \simeq Z_N^* \times Z_M^*$ for $\gcd(M, N) = 1$. An important practical consequence of the CRT is the possibility to do computations with smaller numbers and thus to reduce the running time of algorithms in certain situations (e.g. when decrypting an RSA encrypted message).

(a) Compute all solutions to the quadratic equation $X^2 \equiv 118 \bmod 221$

(b) Find all solutions to $X^2 \equiv 1 \bmod 175$

(c) For $p = 13$ and $q = 19$ set $n = pq$. Let $e = 127$ and $d = e^{-1} \bmod \varphi(n)$. Given $c := 197 = m^e \bmod n$. Determine d and then m via $m = c^d \bmod n$. (this is Textbook-RSA with very small primes :))

Solution:

(a) As $221 = 13 \cdot 17$ we can compute in $\mathbb{Z}_{13} \times \mathbb{Z}_{17}$ instead of solving the equation in $\mathbb{Z}_{221}$. By the Chinese remainder theorem we obtain a pair of equations: $X^2 \equiv 118 \bmod 13$ and $X^2 \equiv 118 \bmod 17$ which are equivalent to $X^2 \equiv 1 \bmod 13$ and $X^2 \equiv 16 \bmod 17$. The first equation has solutions $x_1 = 1$ and $x_2 = -1 = 12$. while the second equation has solutions $y_1 = 4$ and $y_2 = -4 = 13$. The pair of equations in $\mathbb{Z}_{13} \times \mathbb{Z}_{17}$ therefore has four solutions: $\{(1, 4), (1, 13), (12, 4), (12, 13)\}$ which can be mapped back to $\mathbb{Z}_{221}$ via the transformation $(x, y) \mapsto x \cdot (-3) \cdot 17 + y \cdot (4 \cdot 13)$.

(b) We apply the CRT and note that $175 = 7 \cdot 5^2$. We get two equations: $X^2 = 1 \bmod 7$ (with solutions $x_1' = 1$ and $x_2' = 6$) and $X^2 = 1 \bmod 5^2$ with solutions $x_3' = 1$ and $x_4' = 24$). We recombine these solutions (4 possibilities) to get the solutions to the original equation: $x_1 = h^{-1}(1, 1) = 1$, $x_2 = 76$, $x_3 = 99$ and $x_4 = 174$.

(c) d can be determined by the extended euclidean algorithm: $\gcd(e, \varphi(n)) = 1$ and we find $1 = (-17) \cdot e + 10 \cdot \varphi(n)$ thus $d = -17 = 199 \bmod \varphi(n)$. Retrieving m can be done by computing $197^d \bmod n$ but the numbers are rather large and therefore we rather apply the CRT to compute in $\mathbb{Z}_p \times \mathbb{Z}_q$ instead of $\mathbb{Z}_n$.

We have $c = 197 \equiv_{19} 7$ and $d = 199 = \equiv_{18} 1$ (reducing the exponent), thus $197^d = 7 \bmod 19$. Moreover $c = 197 \equiv_{13} 2$ and $d = 199 \equiv_{12} 7$, thus $197^d = 2^7 = 128 = 11 \bmod 13$. Putting it all together again by moving back to $\mathbb{Z}_{13 \cdot 19}$ (note that $3 \cdot 13 - 2 \cdot 19 = 1$) we get: $197^d = 7 \cdot (3 \cdot 13) - 11 \cdot (2 \cdot 19) = -145 = 102 = m$.

Exercise 5.4 φ vs. λ

Let $p = 7$, $q = 11$, and $N = pq$. Furthermore set $e = 7$.

(a) Compute $\varphi(N)$ and $\lambda(N)$.

(b) Compute $e^{-1} \bmod \varphi(N)$ and $e^{-1} \bmod \lambda(N)$.

(c) Compute $\mathbb{Z}_{\varphi(N)}^*$ and $\mathbb{Z}_{\lambda(N)}^*$. How are both groups related to each other?

(d) Prove that for $N = pq$ with $p \neq q$ prime and for any e, $\gcd(e, \varphi(N)) = 1$ if and only if $\gcd(e, \lambda(N)) = 1$.

Solution:

(a) $\varphi(N) = 6 \cdot 10 = 60$ and $\lambda(N) = lcm(6, 10) = 30$.

(b) $e^{-1} = 13 \bmod 30$ and $e^{-1} = 43 \bmod 60$.

(c) $\mathbb{Z}_{30}^* = \{1, 7, 11, 13, 17, 19, 23, 29\}$ and $\mathbb{Z}_{60}^* = \{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59\}$. Hence, $\mathbb{Z}_{\lambda(N)}^*$ is a subgroup of $\mathbb{Z}_{\varphi(N)}^*$ (this also holds in general).

(d) Recall that for natural numbers a, b we have $lcm(a, b) = \frac{ab}{\gcd(a,b)}$. Since $\lambda(N) = lcm(p-1, q-1)$ and $\varphi(N) = (p-1)(q-1)$, we have $\varphi(N) = \gcd(p-1, q-1) \cdot \lambda(N)$. Thus, if $\gcd(e, \varphi(N)) = 1$ then for sure $\gcd(e, \lambda(N)) = 1$.

On the other hand, since $\lambda(N) | \varphi(N)$, we have $\mathbb{Z}_{\lambda(N)}^* \leq \mathbb{Z}_{\varphi(N)}^*$. Hence $e \in \mathbb{Z}_{\lambda(N)}^* \Rightarrow e \in \mathbb{Z}_{\varphi(N)}^*$.

Exercise 5.5 **Structure of $\mathbb{Z}_N$**

Show that:

(a) $a \in \mathbb{Z}_N$ is a generator of $\mathbb{Z}_N$ iff $a \in \mathbb{Z}_N^*$.

(b) $\langle a \rangle = \langle \mathsf{gcd}(a, N) \rangle$ for any $a \in \mathbb{Z}_N$.

(c) There are exactly $\varphi(m)$ elements of order m in $\mathbb{Z}_N$. In particular conclude: $\sum_{m|N} \varphi(m) = \varphi(N)$.

(d) $\langle \mathsf{lcm}(a, b) \rangle = \langle a \rangle \cap \langle b \rangle$ for any $a, b \in \mathbb{Z}_N$.

Solution:

(a) Recall how to test if a given group element is a generator:

$$\langle g \rangle = \mathbb{G} \text{ iff } \forall p \mid |\mathbb{G}| : g^{\frac{|\mathbb{G}|}{p}} \neq 1.$$

or put in another way:

$$\langle g \rangle \neq \mathbb{G} \text{ iff } \exists p \mid |\mathbb{G}| : g^{\frac{|\mathbb{G}|}{p}} = 1.$$

In our case we have $\mathbb{G} = \mathbb{Z}_N$, so exponentiation becomes multiplication and $|\mathbb{G}| = N$:

$$\langle g \rangle \neq \mathbb{Z}_N \text{ iff } \exists p \mid N : g \cdot \frac{N}{p} \equiv_N 0.$$

This means, for $g \in \mathbb{Z}_N$ to be a generator of $\mathbb{Z}_N$ there must not be any prime p which divides N and g at the same time (otherwise $\frac{g}{p}$ would be a natural nunmber so that $\frac{gN}{p} \equiv_N 0$); but this means that the only divisor common to both g and N can be 1, that is, g and N have to be coprime or short $g \in \mathbb{Z}_N^*$.

In particular, $\mathbb{Z}_N$ has exactly $\varphi(N) = |\mathbb{Z}_N^*|$ many generators.

(b) Obviously $a \cdot \frac{N}{\mathsf{gcd}(a,N)} \equiv_N 0$, as $\mathsf{gcd}(a, N) \mid a$. Thus $|\langle a \rangle|$ divides $\frac{N}{\mathsf{gcd}(a,N)}$.

By definition we have $|\langle a \rangle| \cdot a \equiv_N 0$, i.e. there is some $k \in \mathbb{N}$ s.t. $|\langle a \rangle| \cdot a = k \cdot N$.

Dividing both sides by $\gcd(a, N)$ yields $|\langle a \rangle| \cdot \frac{a}{\mathsf{gcd}(a,N)} = k \cdot \frac{N}{\mathsf{gcd}(a,N)}$, that is, $\frac{N}{\mathsf{gcd}(a,N)}$ divides $|\langle a \rangle| \cdot \frac{a}{\mathsf{gcd}(a,N)}$.

But as $\frac{N}{\mathsf{gcd}(a,N)}$ cannot divide $\frac{a}{\mathsf{gcd}(a,N)}$ anymore, $\frac{N}{\mathsf{gcd}(a,N)}$ has to divide $|\langle a \rangle|$, in other words, $|\langle a \rangle|$ has to be a multiple of $\frac{N}{\mathsf{gcd}(a,N)}$.

So $|\langle a \rangle| = \frac{N}{\mathsf{gcd}(a,N)}$.

(b) As a is a multiple of $\mathsf{gcd}(a, N)$ we have $\langle a \rangle \subseteq \langle \mathsf{gcd}(a, N) \rangle$.

Note that $|\langle \mathsf{gcd}(a, N) \rangle| = \frac{N}{\mathsf{gcd}(a,N)}$.

Let $k := |\langle a \rangle|$. Then $N \mid ak$. Canceling $\mathsf{gcd}(a, N)$ in both a and N yields therefore that $\frac{N}{\mathsf{gcd}(a,N)} \mid k$. As $k \geq 1$, this means that $k = \frac{N}{\mathsf{gcd}(a,N)}$. So the claim follows.

(c) From (b) it follows that any $a \in \mathbb{Z}_N$ generates a subgroup of order exactly $\frac{N}{\mathsf{gcd}(a,N)}$, and this subgroup is also generated by $\mathsf{gcd}(a, N)$.

So, for any two elements a, b of the same order m, we have

$$\frac{N}{\mathsf{gcd}(a, N)} = |\langle a \rangle| = m = |\langle b \rangle| = \frac{N}{\mathsf{gcd}(b, N)}.$$

This means: $\mathsf{gcd}(a, N) = \frac{N}{m} = \frac{N}{\mathsf{gcd}(b,N)}$, in particular, $\langle a \rangle = \langle \frac{N}{m} \rangle = \langle b \rangle$.

Hence, there is exactly one subgroup of order m for any $m \mid N$ which is generated by $\frac{N}{m}$; this subgroup is isomorphic to $\mathbb{Z}_m$, and has by virtue of (a) exactly $\varphi(m)$ many generators, that is, elements of order m.

In other words: $\sum_{m|N} \varphi(m) = \varphi(N)$.

(d) As shown in (c) we may assume that a and b divide N – otherwise replace a by $\mathsf{gcd}(a, N)$ and b by $\mathsf{gcd}(b, N)$.

Remark: $\langle a\rangle \cap \langle b\rangle$ is also a subgroup of both $\langle a\rangle$ and $\langle b\rangle$: 1 is included in both, and for $x, y \in \langle a\rangle \cap \langle b\rangle$ we have $x+y \in \langle a\rangle$ and $x + y \in \langle b\rangle$, thus also $x + y \in \langle a\rangle \cap \langle b\rangle$). As any subgroup of a cylcic group is cyclic again, $\langle a\rangle \cap \langle b\rangle$ has to cyclic.

Thus, there is some divisor d of N (recall (c)) such that $\langle d\rangle = \langle a\rangle \cap \langle b\rangle$.

As $\langle d\rangle$ is a subgroup of both $\langle a\rangle$ and $\langle b\rangle$, we have that $|\langle d\rangle|$ divides both $|\langle a\rangle|$ and $|\langle b\rangle|$.

By virtue of (c) this can also be stated as: $\frac{N}{d}$ divides both $\frac{N}{a}$ and $\frac{N}{b}$, in other words, there are integers x, y s.t.

$$x\frac{N}{d} = \frac{N}{a} \wedge y\frac{N}{d} = \frac{N}{b}, \text{ i.e. } d = xa = yb$$

i.e. d is a common multiple of a and b, in particular $\mathsf{lcm}(a, b) \mid d$.

Using again (c) this implies that

$$|\langle d\rangle| = \frac{N}{d} \leq \frac{N}{\mathsf{lcm}(a, b)}.$$

On the other hand we have $\mathsf{lcm}(a, b) \in \langle a\rangle \cap \langle b\rangle = \langle c\rangle$ and $|\langle \mathsf{lcm}(a, b)\rangle| = \frac{N}{\mathsf{lcm}a,b}$– as a and b both divide N, also $\mathsf{lcm}(a, b)$ divides N, so $\mathsf{gcd}(\mathsf{lcm}(a, b), N) = \mathsf{lcm}(a, b)$.

Hence, $d = \mathsf{lcm}(a, b) \pmod{N}$.