Cryptography, winter 2006

PROF. DR. WERNER SCHINDLER, DIPL.-INF. DANIEL LOEBENBERGER

8. Exercise sheet (17.01.2007)
Hand in solutions to the homework exercises
on Wednesday, January 31st, in the tutorial/the lecture.

Exercise 8.1 (Fast exponentiation). *We consider the fast expoinentiation routine from the lecture.*

- *Compute* $81^{27} \pmod{100}$.
- *Show that the algorithm computes* $x^e \pmod{m}$ *in* $\mathcal{O}(\log e)$ *operations in* $\mathbb{Z}_m$.
- *Which problems arise when you want to compute* x^e *for large* e *over* $\mathbb{Z}$*?*

Exercise 8.2 (Order and Carmichael numbers).

A Fermat witness *is a number* $a \in \mathbb{Z}_n$ *satisfying* $a^{n-1} \not\equiv 1 \pmod{n}$. *During a Fermat test such a number proves that a number* n *is composite.*

A Carmichael number *is a composite number* n *satisfying* $x^{n-1} \equiv 1 \pmod{n}$ *for all* $x \in \mathbb{Z}_n^\times$. *Carmichael number are exactly those numbers for which there exist no Fermat witnesses, although they are not prime. The Fermat test will always answer 'probably prime' for these numbers, in spite of the fact that they are composite. Note for any* $a \in \mathbb{Z}_n$ *with* $\gcd(a, n) \neq 1$, *we have* $a^{n-1} \not\equiv 1 \pmod{n}$.

The multiplicative order $\mathrm{ord}_n(x)$ of x modulo n *is the smallest natural number* e *greater zero satisfying* $x^e \equiv 1 \pmod{n}$. *This is just the order of* $x \bmod n$ *in the group* $\mathbb{Z}_n^\times$. *Lagrange's theorem states that the order* $\mathrm{ord}_n(x)$ *of* x *modulo* n *is always a divisor of* $\varphi(n)$.

(i) *Let* n *and* M *be coprime. Let* e *be the order of* x *modulo* n *and* f *the order of* x *modulo* M. *Show: The least common multiple* $\mathrm{lcm}(e, f)$ *of* e *and* f *is the order of* x *modulo* $n \cdot M$.

(ii) *Compute the (multiplicative) order of* 3 *modulo* 100.

(iii) *Generalize (i) to more coprime factors* $n_1 \cdot \ldots \cdot n_r$ *and compute the (multiplicative) order of* 3 *modulo* 100100.

(iv) *Show that* $561 = 3 \cdot 11 \cdot 17$ *is a Carmichael number, i.e. for every comprime* a *to* 561 *we have:* $a^{560} \equiv 1 \pmod{561}$.

Exercise 8.3 (Miller-Rabin-Test (also known as strong primality test)). *We have seen that for the Fermat test there are composite numbers n for wich the Fermat test answers 'probably prime' for all choices of $a \in \mathbb{Z}_n^\times$. In this exercise we will consider an improvement of the Fermat test:*

Algorithm. Strong primality test.

Input: An odd number $n = 1 + 2^s t$ with t odd and an integer $a \in \mathbb{Z}_n^\times$.
Output: Either 'n is a strong probable prime base a' or 'n is composite'.

1. $b \leftarrow a^t \pmod n$;
2. If ($b == 1$ or $b == n - 1$) then
3. Return 'n is a strong probable prime base a';
4. For $j = 1, \ldots, s - 1$ do 5–7
5. $b \leftarrow b^2 \pmod n$;
6. If ($b == n - 1$) then
7. Return 'n is a strong probable prime base a';
8. Return 'n is composite';

- *Discuss the above algorithm. Why is the test stronger than the Fermat test?*

Exercise 8.4 (Homework: Strong primality test, implementation). (10 points)

10

Implement the strong primality test (Miller-Rabin test) in a programming language of your choice. The program shall ask for an integer n and a number of rounds k and apply the strong primality test k times with randomly choosen bases $a \in \mathbb{Z}_n^\times$ and return either 'composite' or 'probable prime'.

- Find the smallest composite strong pseudoprime to the base 2, 3 and 5, respectively.

  Solution. The pseudoprimes are 2047 (base 2), 121 (base 3) and 781 (base 5). ◯

- Find the smallest composite number that is simultaneously a strong pseudoprime to the bases 2 and 3.

  Solution. The desired pseudoprime is $n := 1373653$. However n is not a strong pseudoprime base 5! ◯

Hand in these numbers and the (commented) source code.

Exercise 8.5 (Homework: Primality testing). (4 points)

4

Which of the two integers $10^{200} + 349$ and $10^{200} + 357$ is probably prime and which is certainly composite? You may use a computer algebra system to find this out. Warning: Not every exponentiation routine is suited for solving this task.

Solution. The number $a := 10^{200} + 349$ is certainly composite since $2^{a-1} \not\equiv 1 \pmod{a}$. The number $10^{200} + 357$ is probable prime, since it passes 100 rounds of the strong pseudoprime test. ◯

Exercise 8.6 (Homework: Finding prime numbers). (6 points)

Find a 20 decimal digit prime. Explain how you obtained it and why you believe it is prime. 6

Solution. The smallest 20 decimal digit prime is 10000000000000000051. It was obtained using a 100-rounds strong primality test. The probability that this number is composite (under the fact that the Miller-Rabin test answered 100 times "probable prime" in succession) is $\leq 2^{-100}$. That's why I believe this number is prime.[1] ◯

[1] To be precise the bound is even better, namely $\leq 2^{-200}$. The proof of this fact is, however, quite tricky.