Cryptography

PROF. DR. JOACHIM VON ZUR GATHEN, KONSTANTIN ZIEGLER

4. Assignment: RSA, expected value, Dixon's random squares, and smooth numbers

(Due: **Thursday**, 26 November, 23^{59})

Exercise 4.1 (RSA for non-invertible messages). (6 points)

In the lecture we proved that "RSA works" for messages $m \in \mathbb{Z}_N^\times$, meaning that the decryption of an encrypted messages returns the message itself. This is also true for messages $m \in \mathbb{Z}_N \setminus \mathbb{Z}_N^\times$. Prove it. $\boxed{6}$

Hint: Use the Chinese Remainder Theorem to transform a congruence modulo N into a system of two congruences modulo p and q.

Exercise 4.2 (Expected value and the birthday paradox). (12 points)

Given a discrete random variable X, for example the result of a single roll of a fair die. The values that X can take are denoted by x_i and the respective probability is given by $\text{prob}(X = x_i)$. For the example, the x_i are taken from the set $\{1, 2, 3, 4, 5, 6\}$ with each $\text{prob}(X = x_i) = 1/6$.

We are interested in the *expected value* $E(X)$ defined as

$$E(X) = \sum_i x_i \cdot \text{prob}(X = x_i).$$

In the example above, this returns as the expected value for the roll of a single die

$$E(X) = \sum_{1 \le i \le 6} i \cdot \frac{1}{6} = \frac{21}{6} = 3.5.$$

Next, we roll the die until a certain number, say "2", appears *for the first time*. The random variable Y is now the *number of rolls* that are performed, until this happens.

(i) What is $\text{prob}(Y = i)$, i.e. the probability that "2" appears for the first time in the ith roll? $\boxed{2}$

(ii) Prove that $E(Y) = 6$. (You may have use for the generalization of the formula for the geometric series $\sum_{k=n}^{\infty} q^k = q^n/(1-q)$ for $q < 1$.) $\boxed{4}$

(iii) Generalize the preceding steps to prove the more general proposition $\boxed{3}$

Proposition. *Suppose that an event A occurs in an experiment with probability p, and we repeat the experiment with independent random choices until A occurs. Then the expected number of executions until A happens is $1/p$.*

Finally, we turn to the birthday paradox.

3 (iv) Compute the probability that in a group of 23 randomly chosen people, (at least) two have the same birthday. Provide a meaningful formula to justify your computation. (You may assume, that birthdays are evenly distributed among 365 days in a year.)

Exercise 4.3 (Dixon's random squares). (16 points)

4 (i) Let $N = q_1 q_2 \cdots q_r$ be odd with pairwise coprime prime power divisors q_i and $r \geq 2$. Show: The equation $x^2 - 1 = 0$ has exactly 2^r solutions in $\mathbb{Z}_N^\times$.

Hint: Use the Chinese Remainder Theorem.

Hint: Prove first, that for prime powers q the equation $x^2 - 1 = 0$ has exactly 2 solutions in $\mathbb{Z}_q$.

3 (ii) Let S be the set of all (s, t) in $\mathbb{Z}_N^2$ with $s^2 = t^2$ in $\mathbb{Z}_N$. Prove that for uniformly randomly chosen (s, t) the probability for $s \not\equiv \pm t \bmod N$ is at least $1 - 2^{1-r}$.

4 (iii) Find a factor of $N = 1517 = 37 \cdot 41$ using Dixon's random squares method. Choose $B = 5$ and execute the algorithm step by step.

1 (iv) For $N = 1845314859041$ compute the value $B = \exp(\sqrt{\ln N \ln \ln N})$ derived in the lecture as well as the promised value $B = \exp(\sqrt{\frac{1}{2} \ln N \ln \ln N})$.

4 (v) Run Dixon's random squares repeatedly on $N = 1845314859041$ with $B = 320$. Hand in a protocol of a *unsuccessful* attempt that does not find a factor. Give a short comment about what has happened.

Exercise 4.4 (Smooth numbers). (5 points)

For Dixon's random squares method B-smooth numbers were important. Denote by $\psi(x, B)$ the number of positive integers less than or equal to x whose prime divisors are at most B. *Dickman's rho function* $\varrho(x, B) = \psi(x, B)/x$ denotes the fraction of B-smooth integers.

1 (i) How many 2-smooth numbers are there up to 100? [This is $\psi(100, 2)$.]

2 (ii) How many 3-smooth numbers are there up to $10\,000$? [This is $\psi(10\,000, 3)$.]

In the lecture we learned that $\varrho(x, B) \approx u^{-u}$ with $u = \ln(x)/\ln(B)$.

(iii) Compute the estimate xu^{-u} of 3-smooth numbers less than $10\,000$ and the relative error of this estimate. Compare to (ii). 2