MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2005
June 9, 2005

Cryptography

Problem Sheet #8

Problem 29

a) Let $N = pq$ be the product of two odd primes $p \neq q$. Show that exactly one fourth of the elements of $(\mathbb{Z}/N)^*$ are squares and that every square in $(\mathbb{Z}/N)^*$ has exactly four square roots.

b) Find all square roots of 210 modulo 9991.

Problem 30

Let $N \geq 9$ be an odd composite integer and let $p_1, \ldots, p_r$ be the distinct prime divisors of N. We define the following subgroups of $(\mathbb{Z}/N)^*$:

$$\begin{aligned} A_N &:= \{x \in (\mathbb{Z}/N)^* : x^{N-1} = 1\}, \\ B_N &:= \{x \in (\mathbb{Z}/N)^* : x^{(N-1)/2} = 1\} \\ C_N &:= \{x \in (\mathbb{Z}/N)^* : x^{(N-1)/2} = \left(\frac{x}{N}\right)\} \end{aligned}$$

a) Show that

$$\begin{aligned} \#A_N &= \prod_{i=1}^{r} \gcd(N-1, p_i - 1), \\ \#B_N &= \prod_{i=1}^{r} \gcd(\frac{N-1}{2}, p_i - 1). \end{aligned}$$

b) Prove

$$[B_N : B_N \cap C_N] \leq 2, \qquad [C_N : B_N \cap C_N] \leq 2$$

and deduce

$$\#C_N = \gamma_N \cdot \#B_N \quad \text{with } \gamma_N \in \{\tfrac{1}{2}, 1, 2\}.$$

Problem 31

Let q be an odd prime such that $p := 2q - 1$ is also prime. Define $N := pq$. Show that

$$\#C_N = \frac{\varphi(N)}{4}.$$

Problem 32

a) Let $N > 7$ be an odd integer such that $x^{(N-1)/2} \equiv 1$ for all $x \in (\mathbb{Z}/N)^*$. Show that N is not prime and that $\left(\frac{x}{N}\right) = -1$ for half of the elements of $(\mathbb{Z}/N)^*$.

b) Determine all integers $N < 2000$ with the property described in a).

Due: Thursday, June 16, 2005, 14:10 h