REDUCTION OF FACTORING TO ORDER FINDING

1. background

We are trying to reduce the problem of factoring $N = pq$ to the problem of finding the order Ord_N of a number y co-prime to N. We have seen in class that if we can find a number y which is co-prime to N, and such that $r = Ord_N(y)$ is even and also $y^{r/2} \neq -1$, we can find a non-trivial factor for N. We thus want to show that a random y would satisfy these conditions with good probability.

2. Proof

We prove the following lemma:

Lemma 1. *Pick a random number y co-prime to N, namely, a random element of Z_N^*. Denote by r the order of y. Then*

$$Pr(r \text{ even } \& \ \mathrm{y}^{\mathrm{r}/2} \neq -1) \geq 3/4$$

We prove the lemma using the following claim.

Claim 1. *Let p be an odd prime. Let 2^d be the largest power of 2 that devides $p-1$ (the size of the group Z_p^*). Then if we pick a random number z in Z_p^*, with probability exactly half 2^d devided the order of z.*

Proof. $d \geq 1$ since p is odd. Since Z_p* is cyclic, let g be a generator. Picking a random number in Z_p^* is like picking a random k between 1 and $p-1$ and setting $z = g^k$. If k is odd, which happens with probability half, then we have that $g^{kOrd_p(z)} = z^{Ord_p(z)} = 1$, and since the order of g is $p-1$ we have $p-1|kOrd_p(z)$ which implies that 2^d devides $Ord_p(z)$ (using the fact that k is odd). If k is even we have that $g^{k(p-1)/2} = (g^{p-1})^{k/2} = 1$, and so $Ord(g^k) = Ord(z)$ devides $(p-1)/2$ and so cannot be devided by 2^d. □

We can now prove the lemma. We know by the Chinese remainder theorem that choosing a random y in Z_N^* is equivalent to choosing two random numbers $0 < a_p < p, 0 < a_q < q$ (y would then satisfy the equations $y = a_p \mod p, y = a_q \mod q$.)

Set $r_p = Ord_p(a_p), r_q = Ord_q(a_q)$. Set d_p to be the largest power of 2 that devides r_p, and likewise d_q is the largest power of 2 that devides r_q. By the previous claim, it follows that the probability that $d_p = d_q$ is at most 1/4.

It is easy to see that $r_p|r$: This is because $a_p^r = y^r = 1$ modulo p. Likewise, $r_q|r$. Hence, if r is odd, this means that r_p and r_q are both odd, which means that $d_p = d_q$.

Also, if r is even, and $y^{r/2} = -1 \mod N$, then $y^{r/2} = -1 \mod p$. Hence, r_p cannot devide $r/2$. But r_p does devide r! This means that d_p must be equal to the largest power of 2 that devides r. But the same argument works for d_q, and so in this case too we get that $d_p = d_q$.

Hence, we get that

$$Pr(r \text{ is odd, OR } \mathrm{y}^{\mathrm{r}/2} = -1 \mod \mathrm{N}) \leq \mathrm{Pr}(\mathrm{d_p} = \mathrm{d_q}) \leq 1/4$$

and this completes the proof.