

Factoring methods (numbers from nature, not RSA)

1. Small factors: (a) trial division in fast arith
($p < 10^4$, $p < 2^{31}$)

- (b) Pollard rho (best algorithm):

Finds small prime factor p of large number n using

$$x_0 = 2, x_{j+1} = x_j^2 + 1 \pmod n$$

Values of polyn $x^2 + 1 \pmod p$ (for unknown p)

randomly distributed, by “birthday paradox” expect
a match $x_{2J} = x_J \pmod p$, so a factor

$$p = \gcd(x_{2J} - x_J, n),$$

after \sqrt{p} steps.

- (c) ECM (best method for medium-sized factors)

Look for an elliptic curve $E \pmod p$ with an easy
discrete log problem. Need order(E) with

STEP 1: only small prime factors p_i , or,

STEP 2: only one large prime factor q
(current practice: $p_i < 8000000$, $q < 10^{11}$)