

Let's look more at the group structure of  $(\mathbb{Z}/n\mathbb{Z})^\times$ :

Prop ~~the 2-torsion~~ For odd  $n$ , the 2-torsion subgroup is



$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \underbrace{\{\pm 1\}}_{\substack{\text{in} \\ (\mathbb{Z}/n\mathbb{Z})^\times}} \times \dots \times \underbrace{\{\pm 1\}}_{\substack{\text{in} \\ C_{\phi(p_i^{e_i})}}}$$

$\nwarrow \quad \nearrow$   
cyclic groups of even order

Prop assume that  $n$  is an odd Carmichael number,

~~the~~  $n-1 = 2^r \cdot s$  with  $r \geq 1$  and  $s$  odd.

Then, the set

~~$$T := \{ a \in (\mathbb{Z}/n\mathbb{Z})^\times \mid a^s \equiv 1 \pmod{n} \text{ or } a^{z^i s} \equiv -1 \pmod{n}, a^{z^i s} \equiv 1 \pmod{n} \text{ for some } i \in \{1, \dots, r\} \}$$~~

is a subgroup of  $(\mathbb{Z}/n\mathbb{Z})^\times$ .

For  $0 \leq j \leq r$ , consider the ~~subset~~ subgroup

$$T_j := \{ a \in (\mathbb{Z}/n\mathbb{Z})^\times \mid a^{z^j s} \equiv 1 \pmod{n} \}$$

Clearly,  $T_r = (\mathbb{Z}/n\mathbb{Z})^\times$ , but  $-1 \notin T_0$ . Let  $l$  be the largest index

with  $T_l \neq (\mathbb{Z}/n\mathbb{Z})^\times$ . Consider the subgroup  $U := \{ a \in (\mathbb{Z}/n\mathbb{Z})^\times \mid a^{z^l s} \equiv \pm 1 \pmod{n} \}$ .  
( $z^l s$  is the smallest nr. s.t.  $\phi(p_i^{e_i}) \mid z^l s$  for all  $i$ .)

Lemma 15.6 ~~Prop~~ Let  $n$  be an odd Carmichael number. We have

$$U = (\mathbb{Z}/n\mathbb{Z})^\times \text{ if and only if } n \text{ is prime.}$$

pf  $\Leftarrow$   $a^{z^{l+1}s} \equiv (a^{z^l s})^z \equiv 1 \Rightarrow a^{z^l s} \equiv \pm 1$

$\Rightarrow$  For some  $i$ , every  $z^{l+1}s$ -th power in  $(\mathbb{Z}/n\mathbb{Z})^\times$  is 1 but  $-1$  is not.  $\Rightarrow$  some  $z^l s$ -th power is  $-1$ .

By the chin. rem. thm., there is some  $a \in (\mathbb{Z}/n\mathbb{Z})^\times$  s.t.

$$a \equiv 1 \pmod{p_i^{e_i}} \quad \forall i \neq i$$

$$\text{and } a^{2^i} \equiv -1 \pmod{p_i^{e_i}}.$$

$$\Rightarrow a^{2^i} \not\equiv \pm 1 \pmod{n}.$$

□

Cor 15.3 There is a Monte Carlo alg. to determine whether  $n$  is prime with false pos. prob.  $\leq \frac{1}{2}$ , no false neg., avg. running time  $\tilde{O}((\log n)^2)$

Alg Pick  $a \in (\mathbb{Z}/n\mathbb{Z})^\times$  uniformly at random.

Compute  $b = a^s$ ,

then  $b^{2^i}$  for  $i = 1, \dots, r$ .

If  $b^{2^r} \not\equiv 1$ , return not prime (not even Carmichael).

If  $b^{2^{i+1}} \equiv 1$  but  $b^{2^i} \not\equiv \pm 1$  for some  $i$ , return not prime.

Otherwise, return (maybe) prime.

Pf False pos. can only occur when  $a \in U \not\subseteq (\mathbb{Z}/n\mathbb{Z})^\times$ . □

(even just for  $i=L$ )

an unconditional

Prmk There is also a deterministic alg. that determines whether  $n$  is prime in time  $\tilde{O}((\log n)^6)$ . (AKS algorithm)

Prmk Assuming the generalised Riemann hypothesis,  $(\mathbb{Z}/n\mathbb{Z})^\times$  is generated by  $1, \dots, \lfloor 3(\log n)^2 \rfloor$ , so it suffices to check  $a = 1, \dots, \lfloor 3(\log n)^2 \rfloor$  for a deterministic primality test (Miller's test).

~~Thm 15.8~~

random number

Thm 15.8 There's an alg. that returns a ~~value~~  $p \in N$  ~~with~~ ~~prob.  $\frac{1}{2k}$~~  in expected time  $\tilde{O}(k \cdot \log^3 N)$  with  $P(p \text{ prime}) = \frac{1}{2k} \cdot \frac{1}{\log N}$ .  
All primes  $p \in N$  are equally likely to occur.

Alg Pick  $p \in N$  uniformly at random. If Rabin-Miller says "prob. prime"  $k$  times, return  $p$ . Otherwise, start over.

Qf The number of primes  $p \in N$  is  $\geq \Omega(\frac{N}{\log N})$ .

$\Rightarrow$  The alg. makes  $\leq O(\log N)$  attempts on average.

On each attempt, the prob. of returning a composite ~~no.~~ is  $\leq \frac{1}{2k}$ .

□

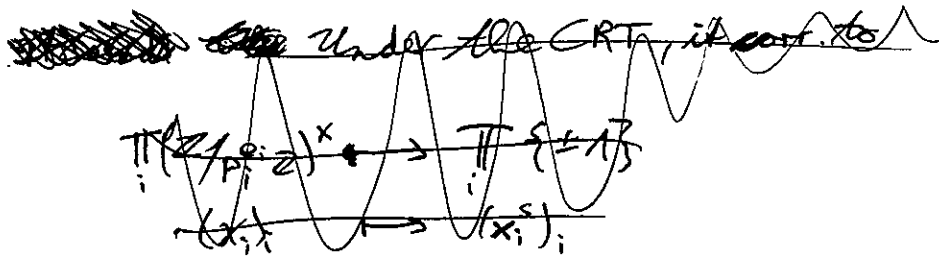
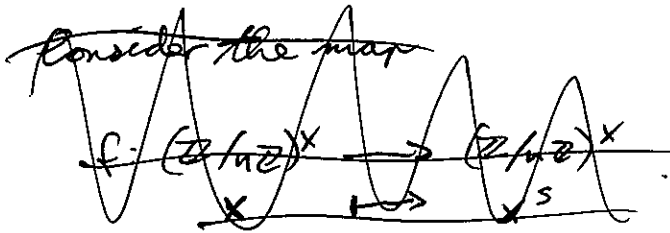
Exer Many alg. that require choosing a random prime  $p$  actually work with ~~composite~~ composite numbers as well:

Either they succeed, or they prove that  $p$  is composite (e.g. when trying to divide by a nonzero noninvertible element of  $\mathbb{Z}/n\mathbb{Z}$ ).

For others, you may need to prove primality.

Lemma 15.89 Let  $n \geq 3$  be an odd composite integer. Given a uniform random element  $a \in (\mathbb{Z}/n\mathbb{Z})^\times$  and its (multiplicative) order  $\text{ord}(a)$  (or the size  $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$ ), we can with prob.  $\geq \frac{1}{4}$  find a proper divisor  $1 < d < n$  of  $n$  in time  $\mathcal{O}((\log n)^2)$ .

pf Write  $\varphi(n) = 2^t s$  and  $\text{ord}(a) = 2^t u$ .  
 ( $\text{ord}(a) \mid \varphi(n) \Rightarrow t \leq t$  and  $u \mid s$ )



claim: ~~of~~ <sup>with prob.  $\geq \frac{1}{4}$</sup>  of the numbers  $d_i = \gcd(a^{2^i u}, n)$  for  $i = 0, \dots, t-1$ , a proper divisor.

pf As before, let  $s_i$  be the smallest nr. s.t.  $2^{s_i} \mid \varphi(p_i^{e_i}) \leq \varphi(n)$ .

Let  $\varphi(p_i^{e_i}) \mid 2^{s_i}$  and let  $j \neq i$ .

~~we have~~  $\Rightarrow$  We have ~~some~~ hom.

$$f_i: (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \rightarrow \{\pm 1\}, \quad f_j: (\mathbb{Z}/p_j^{e_j}\mathbb{Z})^\times \rightarrow \{\pm 1\}$$

$x \mapsto x^{2^{s_i}}$        $x \mapsto x^{2^{s_j}}$

with surjective  $f_i$ .

With prob.  $\frac{1}{2}$ ,  $f_i(a) = -1$  } independent by CRT

With prob.  $\geq \frac{1}{2}$ ,  $f_j(a) = +1$

$\Rightarrow$  With prob.  $\geq \frac{1}{4}$ ,  $\gcd(a^{2^t u} - 1, n)$  is divisible by  $p_i$ , but

not by  $p_j$ . ~~we have~~