

# PRIMES is in P

## Arithmetic at Random

R.G.E. Pinch

Bristol / Cheltenham

Bristol Algorithms Day / 03 March 2008

## Outline

- 1 Primes
  - Some properties of primes
  - PRIMES is in co-NP, NP, co-RP
  - PRIMES is in P: I
  - PRIMES is in P: II
- 2 Randomness properties
  - Character values
  - Modular forms
  - The Riemann zeta function
- 3 Coda

If  $p$  is prime then ...

- (Fermat)  $b^{p-1} \equiv 1 \pmod{p}$  for all  $b$  coprime to  $p$ ;
- (Miller–Rabin)  $p = 2$  or  $p - 1 = 2^r \cdot s$  and the sequence

$$b^s, b^{2s}, \dots, b^{2^r s} = b^{p-1} \pmod{p}$$

starts with 1 or contains  $\dots, -1, 1, \dots$ ;

- (AKS)  $(X + a)^p \equiv X^p + a \pmod{\mathbb{Z}[X]/\langle p, X^r - 1 \rangle}$ .

Call  $p$  a *probable prime* if  $p$  satisfies one of these conditions.

Let  $\pi(x)$  be the number of primes up to  $x$ .

- (PNT)  $\pi(x) \sim \frac{x}{\log x}$
- (PNT)  $\pi(x) = \text{Li}(x) + \text{error}$

The *Riemann hypothesis* is equivalent to the error term being  $O(x^{1/2+\epsilon})$ .

To what extent may we regard the primes as a *random* sequence with local density  $1/\log x$  ?

For example, the Goldbach conjecture (every even number is the sum of two primes) is very probable.

- PRIMES is in co-NP (COMPOSITES is in P)
  - Certificate: a factor.
  - Certificate: a base failing the Miller–Rabin (“strong”) test.
- PRIMES is in NP
  - Certificate: a primitive root modulo  $p$ , together with factors of  $p - 1$  and a recursive certificate of primality of those factors.
- PRIMES is in co-RP
  - Theorem. If  $n$  is not a prime power then at least  $\frac{3}{4}$  of all bases fail the Miller–Rabin (“strong”) test.
  - Certificate: a base failing the Miller–Rabin (“strong”) test.
- PRIMES is in RP
  - Certificate: an abelian variety with smooth order modulo  $p$ .

- Theorem. If the Generalised Riemann Hypothesis is true, then any consecutive  $2(\log p)^2$  numbers generate the multiplicative group modulo  $p$ .
- Corollary. GRH  $\Rightarrow$  PRIMES is in P.
- Without GRH the best we can say is  $p^{1/2\sqrt{e}}$ .

- Theorem. If the order of  $p$  modulo  $r$  is greater than  $(\log p)^2$  and the AKS condition

$$(X + a)^p \equiv X^p + a \text{ in } \mathbb{Z}[X]/\langle p, X^r - 1 \rangle$$

is satisfied for all  $a \leq \sqrt{r} \log p$ , then  $p$  is prime.

- Corollary. The primality of  $p$  may be determined in time  $O((\log p)^{15/2})$ .

The assertion that such an  $r$  exists and is less than  $(\log p)^3$  follows from a theorem that for primes  $q$ , the largest prime factor of  $q - 1$  behaves sufficiently like that of a “random” integer of the same size.

If  $\chi$  is a multiplicative character mod  $p$  then the consecutive values  $\chi(1), \chi(2), \dots$  are not independent. Indeed for *smooth* values of  $a$  the values of  $\chi(a)$  satisfy multiplicative relations: consider  $\chi(1), \chi(2), \chi(3), \chi(4), \chi(6), \chi(8), \chi(9)$ .

However, sufficiently long blocks of  $\chi$  values share properties of randomly distributed points on the circle.

For example,

$$\sum_{x=0}^{p-1} \left( \frac{x^3 + ax + b}{p} \right) = p - t$$

where

$$|t| \leq 2\sqrt{p}.$$

## Character values

- The sequence  $\alpha n \bmod 1$  is uniformly distributed
- The sequence  $\alpha n^d \bmod 1$  is uniformly distributed
- The sequence  $\alpha p \bmod 1$  is uniformly distributed

- The regular graph whose vertices are quaternions of  $p$ -power order and edges correspond to multiplication by prime elements is an expander
- The regular graph whose vertices are supersingular elliptic curves over  $GF(p^2)$  and whose edges are  $\ell$ -isogenies is an expander

- The zeroes of the Riemann zeta function appear to be distributed like the eigenvalues of random Hermitian matrices

## Coda

- Explicit arithmetic examples can simulate random phenomena
- The proofs lie deep (sometimes too deep)
- Wir müssen wissen — wir werden wissen