SUPPLEMENT TO CLASS DESCRIPTIONS—WEEK 2, MATHCAMP 2024

1:10 PM CLASSES

Algorithms for large primes. 🌶🌶 (Zach) $\boxed{\text{TW}\Theta\text{FS}}$ 50 minutes

Much of modern internet security relies on a counterintuitive principle: **testing** whether large numbers are prime is fast, but **factoring** those same numbers is believed to be infeasible, even with state-of-the-art supercomputers and factoring algorithms.

For example, consider this 617-digit number n:

3049393803 9064098204 6257224329 8853574672 1496643781 0821538918 8696453420 2146997229 6758419947 0131652491
3849210517 4158750767 8519631211 9495759970 8592524343 0912930217 3156352106 8467091704 3042905675 3647687903
1227528692 0589276904 8370921428 5585719241 1019900737 7816113198 1122159963 1064596622 5416780223 2291640108
9348914343 2024811908 9653390042 0837116144 9456532221 2395483082 5359910625 7243375192 3565957069 9858976093
3034168762 8457872080 4811538402 6599867498 1094692572 8808367980 5389339036 5915012815 2428549483 2182868787
4342301743 0194193066 8801385061 2219622243 0101198484 7699115272 5406666046 4440567481 0600472360 7644097968
6192546646 5327459.

This number n is **not** prime and $n + 8$ **is** prime, and a typical laptop can **verify** both of these facts in fractions of a second. By contrast, the technology to **factor** n (and numbers like it) into primes likely does not yet exist, and most encrypted communications (in particular, most internet traffic) depends on this fact! The example n above is copied directly from the public certificate that protects `https://www.amazon.com`, but this security could be breached by anyone who can factor n into primes, so Amazon and all of its users rely on this not being feasible.

To factor a large number and/or test whether it is prime, the naïve "trial division" algorithm considers all potential factors individually: "is it divisible by 2? 3? 4? 5? etc.". But for numbers with hundreds of digits, this is way too slow, since the universe will literally suffer heat death before this algorithm makes noticeable progress.

So how is it possible to conclude that a large number (like n) is composite *without* factoring it? How can we be sure that a large number (like $n+8$) is prime *without* testing all of its possible prime factors? We'll explore clever algorithms that enable efficient tests like these, and the elegant underlying number theory.

Topics may include: primality certificates; probable vs provable primes; the Great Internet Mersenne Prime Search; generating large primes; the AKS primality test.

Homework: Recommended.

Class format: Lecture

Prerequisites: Modular arithmetic: should understand modular inverses and Fermat's Little Theorem. I plan *not* to assume or use any knowledge of abstract algebra.

COLLOQUIA

Obtaining freedom via ping pong. (Arya) T$\boxed{\text{W}}\Theta$FS 50 minutes

Groups, like people, are defined by their actions. In this talk, we shall delve into the world of geometric group theory, by studying free groups and thinking about which groups are free. The purpose of this talk is to convince the audience that abstract algebra can also be studied by simply drawing pictures. Arya's meta-goal (as always) is to talk about hyperbolic geometry. All of this somehow relates to ping pong. Some familiarity with groups or linear algebra would be useful, but not necessary. Come to the talk to find out more!