Counting in number theory

Finite cyclic groups

Carl Pomerance, Dartmouth College

Rademacher Lecture 2, University of Pennsylvania
September, 2010

Suppose that G is a group and $g \in G$ has finite order n. Then $\langle g \rangle$ is a cyclic group of order n.

For each $t \in \langle g \rangle$, the integers m with $g^m = t$ form a residue class mod n. Denote it by

$$\log_g t.$$

The discrete logarithm problem is the computational task of finding a representative of this residue class; that is, finding an integer m with $g^m = t$.

Finding a discrete logarithm can be *very* easy. For example, say $G = \mathbb{Z}/n\mathbb{Z}$ and $g = 1$. More specifically, say $n = 100$ and $t = 17$. We are asking for the number of 1's to add in order to get 17. Hmmm.

Let's make it harder: take g as some other generator of $\mathbb{Z}/n\mathbb{Z}$. But then computing $\log_g t$ is really solving the congruence

$$mg \equiv t \bmod n$$

for m, which we've known how to do easily essentially since Euclid.

The cyclic group of order n:

What does this title mean, especially the key word "The"?

Take $G_1 = \mathbb{Z}/100\mathbb{Z}$ and $G_2 = (\mathbb{Z}/101\mathbb{Z})^*$. Both are cyclic groups of order 100. Both are generated by 3. And 17 is in both groups.

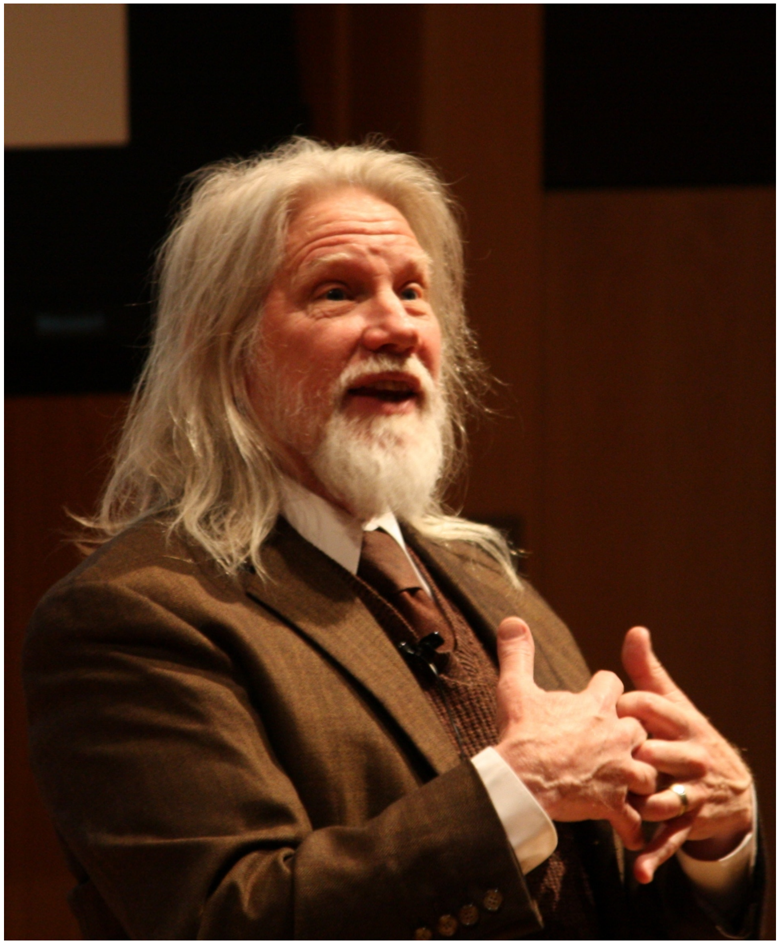
So, there are two versions of computing $\log_3 17$, one in G_1 and one in G_2.

In G_1, we are solving $3m \equiv 17 \bmod 100$. The inverse of 3 is 67, so $m \equiv 17 \cdot 67 \equiv 39 \bmod 100$.

In G_2, we are solving $3^m \equiv 17 \bmod 101$. And this seems much harder.

The moral: when someone talks about *the* cyclic group of a given order, they are not concerned with computational issues.

The algorithmic question of computing discrete logarithms is venerable and also important. Why important?



Whitfield Diffie

Martin Hellman

The Diffie–Hellman key-exchange protocol:

Say we have a cyclic group generated by g, which everyone knows. Alice has a secret integer a and "publishes" g^a. Similarly, Bob has a secret integer b and publishes g^b.

Alice and Bob want to set up a secure session with a secret key that only they know, yet they want to set this up over a public line. Here's how they do it: Alice takes Bob's group element g^b and raises it to her secret exponent a, getting $(g^b)^a = g^{ab}$. Bob arrives at the same group element via a different method, namely $(g^a)^b = g^{ab}$.

Eve (an eavesdropper) knows something's afoot and knows g^a and g^b, but apparently cannot easily compute g^{ab} without finding either a or b, that is without solving the dl problem.

So, a group that is well-suited for cryptographic purposes is one where

- it is easy to apply the group operation;

- it is difficult (in practice) to solve the discrete logarithm problem.

Now let us focus on a different problem, the generators of a finite cyclic group G.

An easy fact: If $G = \langle g \rangle$ and $|G| = n$, then g^j is a generator of G precisely when $(j, n) = 1$. Thus, G has $\varphi(n)$ generators.

Now let's look at the family of groups $(\mathbb{Z}/p\mathbb{Z})^*$, the multiplicative group for a prime p. It is cyclic of order $p-1$ and so has $\varphi(p-1)$ generators.

There are already interesing questions:

- Given a prime p, how easy is it to find a generator for $(\mathbb{Z}/p\mathbb{Z})^*$?

- What is the expected number of random choices from $(\mathbb{Z}/p\mathbb{Z})^*$ until the group is generated?

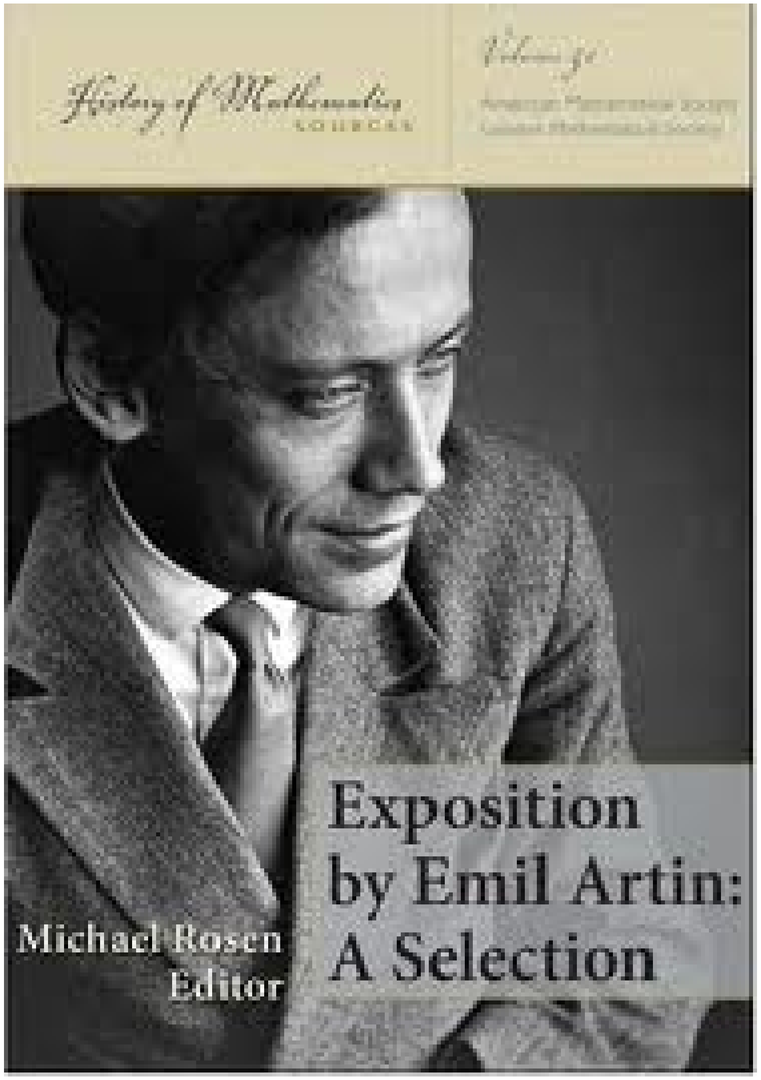
However, I would like to move towards counting problems.

We represent elements of $(\mathbb{Z}/p\mathbb{Z})^*$ with integers, and if "p" is hidden, we may not know exactly which group we are talking about. For example, take the element 10. Do we mean 10 (mod 3), 10 (mod 7), 10 (mod 11), . . . ?

Gauss asked the following question. If you take a prime $p \neq 2, 5$ and convert $1/p$ into decimals, then the decimal is repeating, and the length of the period is a divisor of $p-1$. Is it actually equal to $p-1$ infinitely often?

This question is equivalent to: Do we have $(\mathbb{Z}/p\mathbb{Z})^* = \langle 10 \rangle$ for infinitely many primes p?

Artin's conjecture (1927): *If a is an integer not equal to -1 nor a square, then there are infinitely many primes p with $(\mathbb{Z}/p\mathbb{Z})^* = \langle a \rangle$. In fact, there is a positive constant A_a such that the number of such primes in $[1, x]$ is $(A_a + o(1))\pi(x)$.*


History of Mathematics
SOURCES
Volume 30
American Mathematical Society
London Mathematical Society
Exposition by Emil Artin: A Selection
Michael Rosen
Editor

Even the weak form of Artin's conjecture, which asserts the infinitude of primes p with $(\mathbb{Z}/p\mathbb{Z})^* = \langle a \rangle$ is unsolved, but we have some tantalizing theorems.

Hooley (1967): *Assuming the Riemann hypothesis for algebraic number fields (the "GRH"), Artin's conjecture holds.*

Gupta & Murty, Heath-Brown (1984, 1986): *The weak form of Artin's conjecture holds for every prime value of a, except at most two of them.*

Even so, we still do not know a single value of a for which the weak form holds!

It is not so hard to see why we believe Artin's conjecture to be true.

Let's try it for $a = 2$. For $(\mathbb{Z}/p\mathbb{Z})^* = \langle 2 \rangle$ to hold, 2 should not fail any "q-test" for prime q. Failing means that $q \mid p - 1$ and 2 is a qth power mod p. By the Chebotarev density theorem, the proportion among all primes of primes p which are 1 (mod q) and for which 2 is a qth power is $1/(q^2 - q)$. Thus, we should have the proportion of primes p that never fail; that is, for which $(\mathbb{Z}/p\mathbb{Z})^* = \langle 2 \rangle$, is

$$\prod_{q \text{ prime}} \left(1 - \frac{1}{q^2 - q}\right).$$

This product, known as Artin's constant, is equal to 0.3739558.... Sometimes we need correction factors. For example, if $a = 8$, we also cannot take any prime p that is 1 (mod 3).

When counting up to x one must deal with the Chebotarev theorem when q has some size compared to x; that is, we cannot assume that q is fixed with just $x \to \infty$. This is how the GRH enters the fray.

Consider a totally unrelated problem: How many primes p in $[1, x]$ have $p - 1$ squarefree? Here too p must not fail any q-test, which now means that $q^2 \nmid p - 1$. The proportion of primes p which fail is again $1/(q^2 - q)$, so the proportion of primes p with $p - 1$ squarefree should be exactly Artin's constant. Since this is dealing only with primes in residue classes, sieve methods can be used to resolve the problem of larger q's, and this then becomes an unconditional theorem.

The primes seem to be hogging the spotlight here. What about analogues for the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$? In general this group is not cyclic. Let $\lambda(n)$ denote the order of the largest cyclic subgroup. It is also known as the *exponent* of $(\mathbb{Z}/n\mathbb{Z})^*$, since it is the smallest positive number such that $a^{\lambda(n)} \equiv 1 \pmod{n}$ for every a coprime to n.

Questions:
For which integers a are there infinitely many integers n coprime to a for which the order of a in $(\mathbb{Z}/n\mathbb{Z})^*$ is $\lambda(n)$?
If there are infinitely many n, do they form a positive proportion of the natural numbers?

Let $N_a(x)$ denote the number of integers n in $[1, x]$ where a has order $\lambda(n)$ in $(\mathbb{Z}/n\mathbb{Z})^*$.

Let $\mathcal{E}$ denote the set of integers which are either a power higher than the first power or a square multiplied by -1 or ± 2.

Li (1999): *For each integer $a \in \mathcal{E}$, $N_a(x) = o(x)$.*

Li (1999): *For every integer a, $\liminf N_a(x)/x = 0$.*

Li & P (2003): *Assuming the GRH, for each integer $a \notin \mathcal{E}$, $\limsup N_a(x)/x > 0$.*

Shuguang Li

This unexpected oscillation for $N_a(x)/x$ has an elementary analogue, that is also perhaps unexpected.

Consider a game where I start out giving you n quarters. You either give them all back to me, or you get to keep one of them. Here's how it's played:

You flip all of them, and give me all that land heads.
You flip the remaining coins, and again give me all that land heads.
You continue with this unless you have exactly one quarter left, in which case you get to keep it.

Let P_n be the probability that you get to keep a quarter. What is $\lim P_n$?

Answer: The limit does not exist.

For an integer a with $|a| > 1$, let

$$T_a(x) = \frac{1}{x} \sum_{\substack{n \in [1,x] \\ (n,a)=1}} (\text{order of } a \text{ in } (\mathbb{Z}/n\mathbb{Z})^*).$$

So, here we are not so concerned with the maximal possible order of a, but what happens on average.

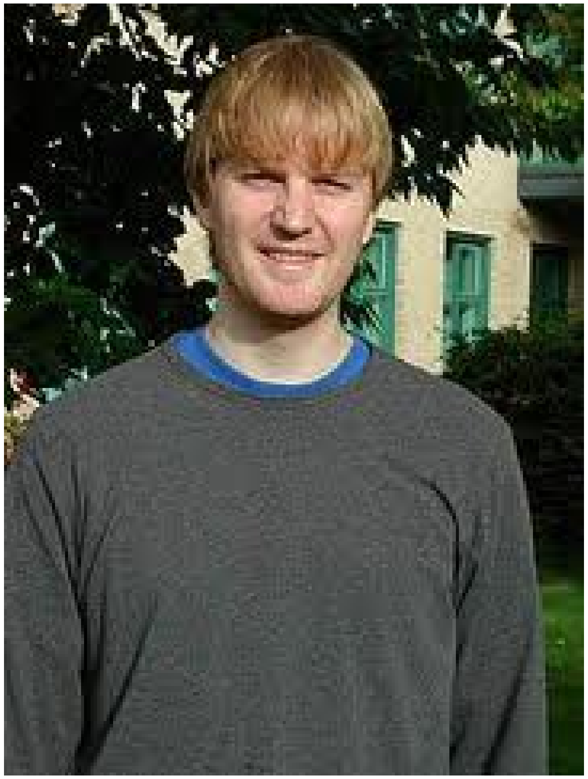
Arnold conjecture (2005): *There is a positive constant* c_a *such that*

$$T_a(x) = (c_a + o(1))\frac{x}{\log x}.$$

Kurlberg & P (2010?): *Arnold is almost right. Specifically, assuming the GRH, there is a positive constant* B*, independent of* a*, such that*

$$T_a(x) = \frac{x}{\log x}\exp\left(\frac{(B + o(1))\log\log x}{\log\log\log x}\right).$$

Vladimir I. Arnold



Pär Kurlberg

Our final counting problem in this lecture has to do with fixed points for discrete logarithms.

Given a prime p, must there be a generator g of $(\mathbb{Z}/p\mathbb{Z})^*$ for which there is some integer $x \in [1, p-1]$ with $\log_g x = x$? That is, $g^x \equiv x \pmod{p}$. If so, say that p has property B.

For example, $2^3 \equiv 3 \pmod{5}$, $3^2 \equiv 2 \pmod{7}$, so that 5 and 7 have property B.

Brizolis (conjecture): *Every prime $p \neq 3$ has property B.*

Lemma. *The prime p has property B, if there is a generator x for $(\mathbb{Z}/p\mathbb{Z})^*$ that is in $[1, p-1]$ and is coprime to $p-1$.*

Proof. If such x exists, say $xy \equiv 1 \pmod{p-1}$ and let $g = x^y$. Then g is a generator for the group and $g^x = x^{xy} \equiv x \pmod{p}$.
□

Let's make this a counting problem. Let $N(p)$ denote the number of generators x for $(\mathbb{Z}/p\mathbb{Z})^*$ that are in $[1, p-1]$ and coprime to $p-1$.

What do we expect for $N(p)$? Well, there are exactly $\varphi(p-1)$ generators in $[1, p-1]$ and exactly $\varphi(p-1)$ integers in this range coprime to $p-1$. If these are "independent events", then we would expect

$$\left(\frac{\varphi(p-1)}{p-1}\right)^2 (p-1) = \frac{\varphi(p-1)^2}{p-1}$$

such numbers. Since $\varphi(n) > cn/\log\log n$, the above expression is at least of order $p/(\log\log p)^2$, which is positive for all large p. Thus, heuristically we have a formula that shows that the Brizolis conjecture holds for all large primes p.

How might we try and prove this?

A venerable tool in analytic number theory for counting is to use characteristic functions.

Say $f_1(g)$ is 1 if $\text{gcd}(g, p-1) = 1$ and 0 otherwise, and $f_2(g)$ is 1 if g is a generator for p and 0 otherwise.

Thus,

$$N(p) = \sum_{g=1}^{p-1} f_1(g) f_2(g).$$

To use this, we need explicit representations for these characteristic functions. Typically in analytic number theory we express a characteristic function as a sum of better-understood quantities, and then reverse the order of summation.

Being coprime to $p-1$ is easy, it is essentially a combinatorial inclusion-exclusion over common divisors of g and $p-1$. We have

$$f_1(g) = \sum_{d \mid \operatorname{gcd}(g, p-1)} \mu(d),$$

where μ is the Möbius function.

Johann Peter Gustav Lejeune Dirichlet, quite the character ...

A combinatorially similar idea works for $f_2(g)$, the characteristic function for generators for p, but here we need to introduce characters. Let γ be some fixed generator for p and let $\zeta = e^{2\pi i/(p-1)}$, a primitive $(p-1)$st root of 1 in $\mathbb{C}$. There is a natural isomophism χ from $(\mathbb{Z}/p\mathbb{Z})^*$ to $\langle\zeta\rangle$ where $\chi(\gamma^j) = \zeta^j$. So, $\chi(g) = \zeta^j$ if $g = \gamma^j$. Then

$$f_2(g) = \sum_{m|p-1} \frac{\mu(m)}{m} \sum_{j=1}^{m} \chi(g)^{j(p-1)/m}.$$

This can be seen by noting that the inner sum is m if $g^{(p-1)/m} \equiv 1 \pmod{p}$ and 0 otherwise.

So,

$$N(p)=\sum_{g=1}^{p-1}\sum_{d\mid \gcd(g,p-1)}\mu(d)\sum_{m\mid p-1}\frac{\mu(m)}{m}\sum_{j=1}^{m}\chi(g)^{j(p-1)/m}.$$

Fine, but are we making any progress? It is perhaps natural to write $g=dh$, use $\chi(g)=\chi(d)\chi(h)$ and rearrange a bit. We have

$$N(p)=\sum_{d,m\mid p-1}\frac{\mu(d)\mu(m)}{m}\sum_{j=1}^{m}\chi(d)^{j(p-1)/m}\sum_{h=1}^{(p-1)/d}\chi(h)^{j(p-1)/m}.$$

Note that the terms in this triple sum with $j=m$ are

$$\sum_{d,m\mid p-1}\frac{\mu(d)\mu(m)}{m}\frac{p-1}{d}=\frac{\varphi(p-1)^2}{p-1}.$$

We have proved that

$$\left|N(p)-\frac{\varphi(p-1)^2}{p-1}\right| \le \sum_{d,m|p-1} \frac{|\mu(d)\mu(m)|}{m} \sum_{j=1}^{m-1} \left| \sum_{h=1}^{(p-1)/d} \chi(h)^{j(p-1)/m} \right|.$$

Let

$$S\left(\chi^{j(p-1)/m}\right) = \max_n \left| \sum_{h=1}^{n} \chi(h)^{j(p-1)/m} \right|,$$

when $1 \le j \le m-1$. Thus,

$$\left|N(p)-\frac{\varphi(p-1)^2}{p-1}\right| \le \sum_{d,m|p-1} \frac{|\mu(d)\mu(m)|}{m} \sum_{j=1}^{m-1} S\left(\chi^{j(p-1)/m}\right).$$

George Pólya

I. M. Vinogradov

The Pólya–Vinogradov inequality

In 1918, Pólya and Vinogradov independently showed that for a nonprincipal character ψ modulo q, we have

$$S(\psi) := \max_n \left| \sum_{h=1}^{n} \psi(h) \right| < cq^{1/2} \log q,$$

for a universal positive constant c. Thus,

$$\sum_{d,m|p-1} \frac{|\mu(d)\mu(m)|}{m} \sum_{j=1}^{m-1} S\left(\chi^{j(p-1)/m}\right) = O(4^{\omega(p-1)} p^{1/2} \log p),$$

where $\omega(n)$ is the number of distinct primes dividing n. Since $\omega(n) = o(\log n)$, we have the above expression being of magnitude at most $p^{1/2+\epsilon}$.

Thus,

$$N(p) = \frac{\varphi(p-1)^2}{p-1} + O(p^{1/2+\epsilon}).$$

Since as we have seen, the main term is at least of order $p/(\log\log p)^2$, this shows that all sufficiently large primes p have $N(p) > 0$.

But is it true for all primes $p \neq 3$?

Questions like this pose a computational challenge, since it involves putting explict constants on all of the inequalities involved. And challenges can remain, since the point at which $N(p) > 0$ is proved to be true may be too large to do a case study up to that point.

Some history: W.-P. Zhang in 1995 gave essentially the above argument but did not work out a starting point for when it is true.

C. Cobelli and A. Zaharescu in 1999 gave a somewhat different proof, showing that $N(p) > 0$ for all $p > 10^{2070}$. They said that a reorganization of their estimates would likely support a bound near 10^{50}.

So, can we do better? And how good is the Pólya–Vinogradov inequality?

It's easy to show via an averaging argument that for χ primitive,

$$S(\chi) \geq \frac{1}{\pi}\sqrt{q}.$$

So, apart from the "$\log q$" factor, the Pólya–Vinogradov inequality is best possible.

We have numerically explicit versions of the Pólya–Vinogradov inequality with reasonable constants, but the Brizolis problem is still difficult to handle completely.

Levin, P, Soundararajan (2010): *The Brizolis conjecture is true.*

To prove this, we skewed the count for $N(p)$. That is, we considered

$$N^*(p) = \sum_{\substack{g \in [1,p-1] \\ g \text{ is a generator} \\ (g,p-1)=1}} \left(1 - \left|\frac{2g}{p-1} - 1\right|\right).$$

instead of

$$N(p) = \sum_{\substack{g \in [1,p-1] \\ g \text{ is a generator} \\ (g,p-1)=1}} 1.$$

A “smoothed” Pólya–Vinogradov inequality:

Let $S_N(\chi) = \max_M \left| \sum_{M \le a \le M+2N} \chi(a) \left(1 - \left|\frac{a-M}{N} - 1\right|\right) \right|$.

Levin, P, Soundararajan (2010): *For χ primitive and $N \le q$, we have $S_N(\chi) \le \sqrt{q} - \frac{N}{\sqrt{q}}$.*

The proof is based on Poisson summation and Gauss sums, and is almost immediate. (A similar result for prime moduli is due to Hua in 1942.)

Mariana Levin

K. Soundararajan

The result is nearly best possible.

Treviño (2010): *For* χ *primitive*, $\max\limits_{N\le q} S_N(\chi) \ge \dfrac{2}{\pi^2}\sqrt{q}$.

Actually, he has a slightly larger constant here, but he favors this one, which has a neat proof. For the value of N that he uses, which is near $q/2$, the upper bound in the LPS theorem is a bit more than twice the Treviño lower bound.

Treviño is now looking at other numerical applications for the smoothed Pólya–Vinogradov inequality.

Enrique Treviño

THANK YOU!