Balanced subgroups of the multiplicative group

Carl Pomerance, **Dartmouth College**
Hanover, New Hampshire, USA

Based on joint work with
Douglas Ulmer

To motivate the topic, let's begin with elliptic curves.

If $a, b \in \mathbb{Q}$ are such that $4a^3 + 27b^2 \neq 0$, the curve

$$y^2 = x^3 + ax + b$$

is nonsingular. In this case the set of rational points on the curve form a finitely generated abelian group, with the group law given by the familiar chord-tangent construction. After Mazur, we know that the torsion part of the group of rational points is universally bounded over all elliptic curves over $\mathbb{Q}$.

However, the rank of the free part of this group (known simply as the rank) may or may not be universally bounded.

The geometric view of the group law on an elliptic curve with rational (or real) coefficients gives formulae for group addition and doubling via calculus and analytic geometry. These formulae continue to make sense even when we have trouble picturing what a chord or a tangent looks like.

Let q be a prime power, say a power of the prime p, and let $\mathbb{F}_q$ be a finite field with q elements. For u an indeterminate, we have the rational function field $\mathbb{F}_q(u)$.

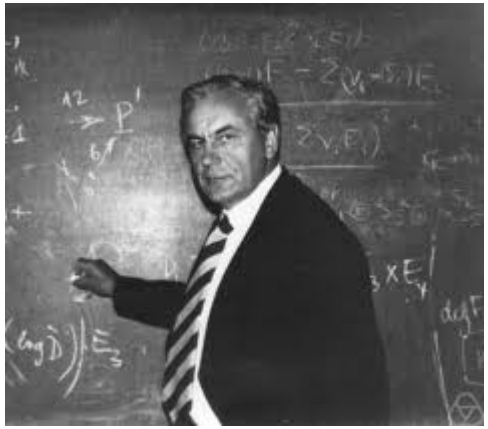
If we consider elliptic curves defined over $\mathbb{F}_q(u)$ and the points on such a curve with coordinates in $\mathbb{F}_q(u)$, then again, we have a finitely generated abelian group. And again we can ask if the rank can be arbitrarily large.

In 1967, Shafarevich & Tate gave a family of elliptic curves over $\mathbb{F}_q(u)$ where the ranks grow arbitrarily large. Their family was considered "isotrivial" meaning that the j-invariant of each curve was in $\mathbb{F}_q$.

In a 2002 Annals paper, Ulmer exhibited a non-isotrivial family, namely

$$y^2 + xy = x^3 - u^d,$$

which has positive-integer parameter d. (The curve is not given here in Weierstrass form.) In particular, for this curve defined over $\mathbb{F}_q(u)$ (of characteristic p), if $d = q^n + 1$, then the rank of the curve is about $q^n/2n$.



I. R. Shafarevich

John Tate

Doug Ulmer

More generally, he showed that if $-1 \in \langle p \bmod d \rangle$, then the rank of $y^2 + xy = x^3 - u^d$ over $\mathbb{F}_q$ is within 4 of

$$\sum_{e|d} \frac{\varphi(e)}{l_q(e)}.$$

Notation: $l_q(e) = |\langle q \bmod e \rangle|$.
So, the fraction $\varphi(e)/l_q(e)$ is just the index of $\langle q \bmod e \rangle$ in $\mathbb{U}_e$.

In the case that $d = q^n + 1$, the hypothesis $-1 \in \langle p \bmod d \rangle$ clearly holds, and each $l_q(e)|2n$, so

$$\sum_{e|d} \frac{\varphi(e)}{l_q(e)} \geq \frac{1}{2n} \sum_{e|d} \varphi(e) = \frac{d}{2n} = \frac{q^n + 1}{2n}.$$

Some natural questions:

- What is the rank on average?
- What is the rank normally?
- Given p, how frequently do we have $-1 \in \langle p \bmod d \rangle$?

Let's begin with the last question, namely, how special is it for d to have the property that $p^n \equiv -1 \pmod{d}$ for some n.

To be specific, lets take $p = 2$ and consider the two sets of integers:

$$S := \{d \ : \ d \mid 2^n - 1 \text{ for some positive integer } n\}$$
$$T := \{d \ : \ d \mid 2^n + 1 \text{ for some positive integer } n\}.$$

Surely they should not be very different!

But they are. For starters, S is just the set of odd numbers, it has asymptotic density $1/2$.

Note that if $r \equiv 7 \pmod{8}$, then r cannot divide any member of T. Indeed, $(2/r) = 1$, so the order of 2 in $\mathbb{U}_r$ divides $(r-1)/2$, which is odd. Hence there can be no n with $2^n \equiv -1 \pmod{r}$. Thus, there can be no member of T divisible by such a prime r.

What can we say about the integers which have no prime factor $r \equiv 7 \pmod 8$?

For any finite set $\mathcal{P}$ of primes, the density of integers not divisible by any member of $\mathcal{P}$ is

$$\prod_{r \in \mathcal{P}} \left(1 - \frac{1}{r}\right).$$

Now suppose that $\mathcal{P}$ runs over all finite subsets of the primes $r \equiv 7 \pmod 8$.

Since

$$\sum_{\substack{r \le x \\ r \equiv 7 \pmod 8}} \frac{1}{r} = \frac{1}{4} \log \log x + O(1),$$

it follows that

$$\prod_{\substack{r \le x \\ r \equiv 7 \pmod 8}} \left(1 - \frac{1}{r}\right) \asymp (\log x)^{-1/4}.$$

In fact, using the fundamental lemma of the sieve, we get that

$$\sum_{\substack{m \le x \\ r|m \Longrightarrow r \not\equiv 7 \pmod 8}} 1 \asymp \frac{x}{(\log x)^{1/4}}.$$

By following these ideas more carefully, one can prove that for p fixed, the number of integers $d \le x$ not divisible by p and for which $-1 \in \langle p \bmod d \rangle$ is $(c_p + o(1))x/(\log x)^{2/3}$, as $x \to \infty$, where c_p is a positive constant. Moree has this worked out in even finer detail as an asymptotic series.

As for the other questions concerning a statistical study of the ranks in this family, there have been some results of P and Shparlinski, and also more recently of Gottschlich.

Pieter Moree

Igor Shparlinski

Avram Gottschlich

Let $R_q(d)$ denote the rank of the elliptic curve $y^2 + xy = x^3 - u^d$ over $\mathbb{F}_q$.

P & **Shparlinski** (2010). *There is an absolute positive constant $\alpha > \frac{1}{2}$ such that*

$$\frac{1}{x} \sum_{d \le x} R_q(d) > x^{\alpha}$$

for all sufficiently large x depending on q. Further,

$$\left(\sum_{\substack{d \le x \\ -1 \in \langle p \bmod d \rangle}} 1 \right)^{-1} \sum_{\substack{d \le x \\ -1 \in \langle p \bmod d \rangle}} R_q(d) \le x^{1 - \log\log\log x/(2\log\log x)}.$$

And for d in a set of asymptotic density 1, we have, as $d \to \infty$,

$$R_q(d) \ge (\log d)^{(\frac{1}{3} + o(1)) \log\log\log d}.$$

Concerning this last result on the normal size of $R_q(d)$, we conjectured something stronger if d was forced to run through the set where $-1 \in \langle p \bmod d \rangle$, namely

Conjecture (P & Shparlinski). *But for $o(x/(\log x)^{2/3})$ choices of $d \le x$ with $-1 \in \langle p \bmod d \rangle$, we have as $x \to \infty$*

$$R_q(d) = (\log d)^{(1+o(1)) \log\log\log d}$$

But it seems we were wrong:

Gottschlich (2012). *Assuming the GRH, but for $o(x/(\log x)^{2/3})$ choices for $d \le x$ with $-1 \in \langle p \bmod d \rangle$, we have as $x \to \infty$*

$$R_q(d) = (\log d)^{(\frac{1}{3} + o(1)) \log\log\log d}.$$

In a more recent paper, Ulmer got a similar formula for the rank for another family of curves: $y^2 = x(x+1)(x+u^d)$. This is (essentially) the Legendre curve. In a very recent preprint, Ulmer, together with Conceição and Hall, extended the set of d's for which the rank formula holds. If we use the notation $R_q(d)$ for the rank, they have shown that for p odd,

$$R_q(d) = \sum_{\substack{e|d \\ \langle p \bmod e \rangle \text{ is balanced}}} \frac{\varphi(e)}{l_q(e)}.$$

So, what does it mean for $\langle p \bmod e \rangle$ to be balanced?

It is a generalization of $-1 \in \langle p \bmod e \rangle$ (when $e > 2$) as we shall now see.

Lady Liberty and the Balanced Scales of Justice

Ricardo Conceição

Chris Hall

Assume $d > 2$. Consider a subgroup H of the unit group $\mathbb{U}_d$. We say H is *balanced* if each coset aH of H in $\mathbb{U}_d$ contains an equal number of elements in $(0, d/2)$ as in $(d/2, d)$.

For example, $H = \mathbb{U}_d$ is a balanced subgroup of $\mathbb{U}_d$.

Also $H = \{1, -1\} = \langle -1 \bmod d \rangle$ is balanced. Indeed, if $a \in \mathbb{U}_d$, then $aH = \{a, -a\}$ and $a, -a$ are in different halves.

If K is a subgroup of $\mathbb{U}_d$ containing a balanced subgroup H, then K too is balanced. Indeed, K is a union of some cosets of H, say $a_1H, \ldots, a_kH$. Then each coset bK is a union of the cosets $ba_1H, \ldots, ba_kH$, and since each of these is split 50-50 between the two halves of $\mathbb{U}_d$, so too is bK split 50-50.

As a corollary, if $-1 \in \langle p \bmod d \rangle$, then $\langle p \bmod d \rangle$ is balanced, as is each $\langle p \bmod e \rangle$ for $e \mid d$, $e > 2$.

However, containing -1 is not the only way for a subgroup of $\mathbb{U}_d$ to be balanced. Here is an interesting family:

Suppose $4 \mid d$. Then $\langle \frac{1}{2}d + 1 \bmod d \rangle$ is balanced.

It's easy to see, since if $a \in \mathbb{U}_d$, then a is odd, so that $\frac{1}{2}da = \frac{1}{2}d$ in $\mathbb{U}_d$. Thus, $a(\frac{1}{2}d + 1) = \frac{1}{2}d + a$, so that a and $a(\frac{1}{2}d + 1)$ lie in different halves of $\mathbb{U}_d$.

Some natural questions:

- Is there a simple criterion for a subgroup H of $\mathbb{U}_d$ to be balanced?

- What are the *minimal* balanced subgroups of $\mathbb{U}_d$? (It means that the subgroup should not contain any balanced proper subgroups.)

- Must a minimal balanced subgroup be cyclic?

- What is the distribution of numbers d such that $\langle p \bmod d \rangle$ is balanced? In particular, are there substantially more of them than for the simpler criterion $-1 \in \langle p \bmod d \rangle$?

For a criterion for a subgroup to be balanced, we turn to Dirichlet characters.

For χ a character modulo d, let

$$c_\chi = \sum_{a \in (0,d/2)} \chi(a).$$

P & Ulmer (2012). *A subgroup H of $\mathbb{U}_d$ is balanced if and only if $c_\chi = 0$ for each odd character χ modulo d which is trivial on H.*

A very simple example: $H = \langle -1 \bmod d \rangle$. There are *no* odd characters modulo d that are trivial on H, so H is balanced.

Lets see how to prove this criterion for a subgroup H of $\mathbb{U}_d$ to be balanced. Let $A = (0, d/2) \cap \mathbb{U}_d$, $B = \mathbb{U}_d \setminus A$. Then H is balanced if and only if

$$f(u) := \#(uH \cap A) - \#(uH \cap B)$$

is identically 0 on $\mathbb{U}_d$. Write

$$f = \sum_{\chi \bmod d} a_\chi \chi, \quad \text{so} \quad a_\chi = \frac{1}{\varphi(d)} \sum_{u \in \mathbb{U}_d} f(u) \chi^{-1}(u).$$

Thus, H is balanced if and only if $a_\chi = 0$ for all $\chi \bmod d$. We check that for χ trivial, a_χ is just the average of $f(u)$ over $\mathbb{U}_d$, so for any H, regardless if it is balanced, we have $a_\chi = 0$.

For χ mod d nontrivial, we work out that

$$a_\chi = \frac{2}{\varphi(d)} \sum_{u \in A} \chi(u) \sum_{h \in H} \chi(h) = \frac{2}{\varphi(d)} c_\chi \sum_{h \in H} \chi(h).$$

Thus, $a_\chi = 0$ if and only if either $c_\chi = 0$ or χ is not trivial on H. Now for χ even and nontrivial, we have $c_\chi = 0$. So we see $a_\chi = 0$ for all χ mod d if and only if $c_\chi = 0$ for all odd χ trivial on H. This is the criterion stated earlier for H to be balanced.

What can be said about $c_\chi = \sum_{a \in (0,d/2)} \chi(a)$ in general?

We noted that if χ is even, then $c_\chi = 0$.

If χ is odd and primitive modulo d, we have that

$$c_\chi \pi i \tau(\bar{\chi}) = L(1, \bar{\chi})(\bar{\chi}(2) - 2)d,$$

where $\tau(\bar{\chi})$ is the Gauss sum, and $L(1, \bar{\chi}) = \sum_{n>0} \bar{\chi}(n)/n$.

In particular, for χ odd and primitive, $c_\chi \neq 0$. As a corollary, if H is balanced in $\mathbb{U}_d$ there cannot be any odd primitive characters modulo d that are trivial on H.

We can work out exactly when $c_\chi \neq 0$. Here χ is an odd character modulo d induced by a primitive character χ' modulo d' (so that d' is the conductor of χ). Then $c_\chi \neq 0$ precisely when both

- Either d/d' is odd or $d \equiv 2 \pmod 4$.

- For each odd prime $\ell \mid d$ with $\ell \nmid d'$, we have $\chi'(\ell) \neq 1$.

That is, H is *not* balanced in $\mathbb{U}_d$ if and only if there is an odd character $\chi \bmod d$ trivial on H induced by a primitive character $\chi' \bmod d'$, with the above bullets holding.

We can use this criterion to enumerate all pairs $H, \mathbb{U}_d$ where H is a balanced subgroup of $\mathbb{U}_d$ and $|H| = n$. In particular, if H does not contain -1 nor $\frac{1}{2}d + 1$ in the case that $4 \mid d$, then there are only finitely many possibilities for pairs $H, \mathbb{U}_d$.

In the case $n = 2$, the only *sporadic* balanced subgroups of order 2 are

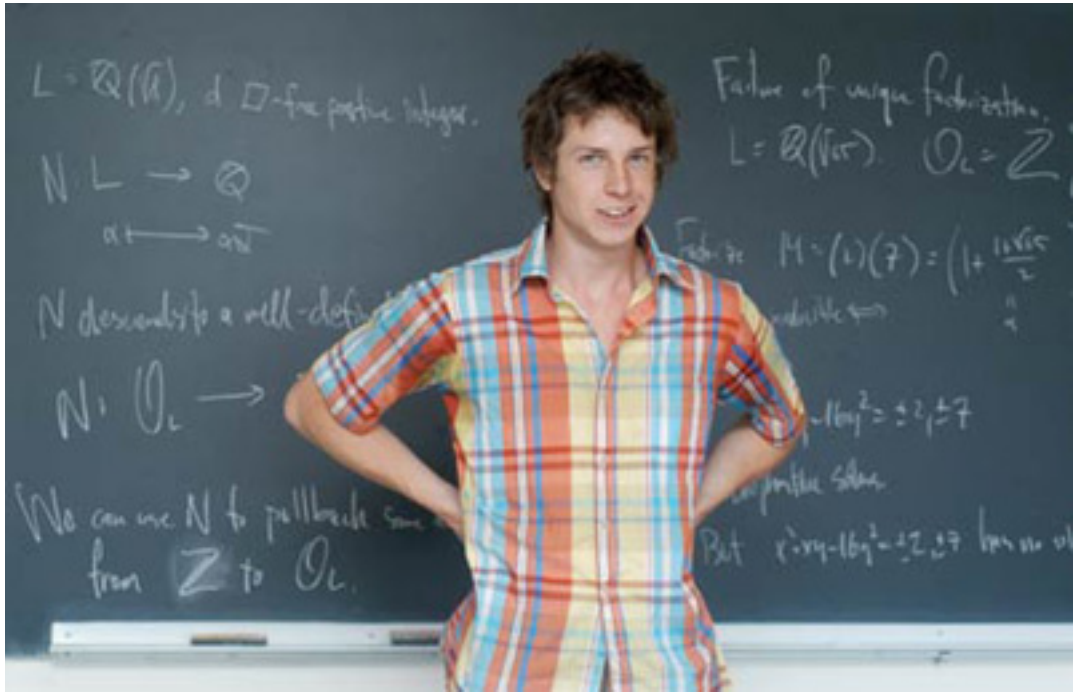
- $d = 24$ and $H = \langle 17 \rangle$ or $\langle 19 \rangle$.

- $d = 60$ and $H = \langle 41 \rangle$ or $\langle 49 \rangle$.

Engberg has enumerated the sporadic balanced subgroups of orders 4, 6, and 8. He found some order 8 minimal balanced subgroups that are not cyclic, so scratch one question!

While the emphasis in the theorem of P & Ulmer is on balanced subgroups of small order, Engberg has considered those of small index, showing for example that for all numbers d, except for a sparse exceptional set, $\mathbb{U}_d$ contains an index-2 sporadic balanced subgroup. Small index examples are common!

Despite the existence of so many sporadic balanced subgroups, P & Ulmer conjecture that for most numbers d for which $\langle p \bmod d \rangle$ is balanced, we have $-1 \in \langle p \bmod d \rangle$ or $4 \mid d$ and $\frac{1}{2}d + 1 \in \langle p \bmod d \rangle$. That is, for a fixed prime p, if $\langle p \bmod d \rangle$ is balanced, it is not sporadic.



Zebediah Engberg

To make the conjecture precise, for a given integer p with $|p| > 1$, let

$$\begin{aligned}
\mathcal{B}_p &= \{d \ : \ (d,p) = 1, \ \langle p \bmod d \rangle \text{ is balanced}\}, \\
\mathcal{B}_{p,0} &= \{d \ : \ 4 \mid d, \ (d,p) = 1, \ \tfrac{1}{2}d + 1 \in \langle p \bmod d \rangle\} \\
\mathcal{B}_{p,1} &= \{d \ : \ (d,p) = 1, \ -1 \in \langle p \bmod d \rangle\}.
\end{aligned}$$

Note that for p even, $\mathcal{B}_{p,0} = \emptyset$ and for p odd, $\mathcal{B}_{p,0} \cap \mathcal{B}_{p,1} = \{4\}$.

For any set $\mathcal{A}$ of integers, let $\mathcal{A}(x) = \mathcal{A} \cap [1, x]$.

P & Ulmer (2012). *If p is odd, then*

$$|\mathcal{B}_{p,0}(x)| \asymp_p \frac{x}{\log\log x}.$$

In all cases, there is a number $\delta_p > 0$ such that

$$|\mathcal{B}_p(x) \setminus \mathcal{B}_{p,0}(x)| = O\left(\frac{x}{(\log x)^{\delta_p}}\right).$$

In particular, if p is odd,

$$|\mathcal{B}_p(x)| = (1 + o(1))|B_{p,0}(x)|$$

as $x \to \infty$.

Conjecture (**P & Ulmer**): *As $x \to \infty$,*

$$|\mathcal{B}_p(x)| = |\mathcal{B}_{p,0}(x)| + (1 + o(1))|\mathcal{B}_{p,1}(x)|.$$

Perhaps it is surprising that there are so many more members of $\mathcal{B}_{p,0}$ (when p is odd) than of $\mathcal{B}_{p,1}$. (Recall that when p is prime, $|\mathcal{B}_{p,1}(x)| \sim c_p x/(\log x)^{2/3}$.)

Why does this happen?

Say p is odd and $d = 2^j m$ is coprime to p and $j \geq 2$. What can we say about

$$v_2(l_p(d)) \text{ ?}$$

(By $v_2(n)$ we mean that number v with $2^v \mid n$ and $2^{v+1} \nmid n$.) Well, we have

$$v_2(l_p(d)) = \max\{v_2(l_p(2^j)),\, v_2(l_p(m))\}.$$

So, what can we say about these two values?

Note that the power of 2 in $l_p(m)$ divides $q-1$ for some prime $q \mid m$, and is usually close to the maximal such power of 2. For most numbers $m \leq x$, this power of 2 is close to $\log\log x$. That is, we usually have

$$2^{v_2(l_p(m))} \approx \log\log x.$$

We also have that $v_2(l_p(2^j)) = j + O_p(1)$.

It is possible to show too that for most numbers m we have $d = 2^j m \in \mathcal{B}_{p,0}$ if and only if $v_2(l_p(2^j)) > v_2 l_p(m)$.

Thus, we obtain a close to necessary and sufficient condition for $d = 2^j m$ to be in $\mathcal{B}_{p,0}$, namely

$$2^j > \log\log x.$$

The distribution of numbers $d = 2^j m$ with $2^j > \log\log x$ is easy, this is of magnitude $x/\log\log x$.

However, in our paper, we sketch a proof that there is *no* positive constant β_p such that

$$|\mathcal{B}_{p,0}(x)| \sim \beta_p \frac{x}{\log\log x}$$

as $x \to \infty$.

We can use our results plus the techniques from the 2010 work of P and Shparlinski to get results on average and normally for $R_q(d)$ for the Legendre curve over $\mathbb{F}_q(u)$. In particular for p an odd prime, we have for almost all $d \in \mathcal{B}_p$ that $R_q(d) = (\log d)^{(1+o(1))\log\log\log d}$ as $d \to \infty$, with the upper bound implicit here depending on the GRH.

Recall the conjecture of P and Ulmer:

$$|\mathcal{B}_p(x)| = |\mathcal{B}_{p,0}(x)| + (1 + o(1))|\mathcal{B}_{p,1}(x)|$$

as $x \to \infty$. We have the order of magnitude for $|\mathcal{B}_{p,0}(x)|$, when p is odd, it is $x/\log\log x$. We have an asymptotic for $|\mathcal{B}_{p,1}(x)|$, it is $c_p x/(\log x)^{2/3}$. Late breaking news:

Engberg: *The conjecture is true, in fact* $|\mathcal{B}_p(x) \setminus (\mathcal{B}_{p,0}(x) \cup \mathcal{B}_{p,1}(x))| = O(x/(\log x)^{2/3+1/1000})$.

The proof involves a careful classification of the sporadic cases, plus some big tools from analytic number theory, including the large sieve and zero density estimates for Hecke L-functions.

THANK YOU