Balanced subgroups of the multiplicative group

Carl Pomerance, Dartmouth College
Hanover, New Hampshire, USA

Based on joint work with
D. 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 projectivized version of the curve, namely

$$\{(u : v : w) \in \mathbb{P}^2(\mathbb{Q}) : wv^2 = u^3 + auw^2 + bw^3\}$$

form an abelian group, with group identity $(0 : 1 : 0)$, the "point at infinity." The group law is found via the familiar chord/tangent construction, and it is a theorem that it is finitely generated. It is not known if the rank of this group can be arbitrarily large.

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 (it's unique up to isomorphism). 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 and 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 $q^n/2n$.

More generally, he showed that if $-1 \in \langle p \rangle_d$ (the notation means that $p^n \equiv -1 \pmod{d}$ for some n), then the rank of $y^2 + xy = x^3 - u^d$ over $\mathbb{F}_q$ is within 4 of

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

Here, the notation $l_q(e)$ stands for the order of q in the unit group modulo e. So, the fraction $\varphi(e)/l_q(e)$ is just the index of $\langle q \rangle_e$ in $\mathbb{U}_e$.

In the case that $d = q^n + 1$, the hypothesis $-1 \in \langle p \rangle_d$ 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 $-1 \in \langle p \rangle_d$?

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

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

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

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

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

Since

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

it follows that

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

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

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

By following these ideas more carefully, one can prove that for p fixed, the number of integers $d \leq x$ not divisible by p and for which $-1 \in \langle p \rangle_d$ is $(c_p + o(1))x/(\log x)^{2/3}$, as $x \to \infty$, where c_p is a positive constant.

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.

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,

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

And for d in 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 $-1 \in \langle p \rangle_d$, namely

Conjecture (P & Shparlinski). *But for $o(x/(\log x)^{2/3})$ choices of $d \le x$ with $-1 \in \langle p \rangle_d$, 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 $-1 \in \langle p \rangle_d$, 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 again use the notation $R_q(d)$ for the rank, they have shown that for p odd,

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

So, what does it mean for $\langle p \rangle_e$ to be balanced?

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

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 $H = \{1, -1\} = \langle -1 \rangle_d$ is balanced. Indeed, if $a \in \mathbb{U}_d$, then a and $-a$ are not both in the same half.

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 $-1 \in \langle p \rangle_d$, then $\langle p \rangle_d$ is balanced, as is each $\langle p \rangle_e$ 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 $\langle \frac{1}{2}d + 1 \rangle$ is balanced in $\mathbb{U}_d$.

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 $\langle p \rangle_d$ is balanced? In particular, are there substantially more of them than for the simpler criterion $-1 \in \langle p \rangle_d$?

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

For a finite abelian group G, a character is a homomorphism from G to the multiplicative group of complex numbers, so necessarily to the group of roots of unity.

A character χ on $\mathbb{U}_d$ may be extended to a *Dirichlet character* modulo d: one takes $\chi(n) = \chi(n \pmod d)$ when $(n, d) = 1$, and $\chi(n) = 0$ otherwise.

The trivial character on $\mathbb{U}_d$ corresponds to the prinicipal character $\chi_{0,d}$ modulo d, which is just the characteristic function of the integers coprime to d.

A character χ modulo d is said to be *induced* by a character χ' modulo d' if $d' \mid d$ and $\chi = \chi'\chi_{0,d}$.

The *conductor* of a character χ modulo d is the smallest d' for which there is a character χ' modulo d' that induces χ.

A character χ modulo d is *primitive* if its conductor is d.

A character χ modulo d is *odd* if $\chi(-1) = -1$ and otherwise it is *even*. Note that an odd character is an odd function, and an even character is an even function.

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: $H = \langle -1 \rangle$ in $\mathbb{U}_d$. There are *no* odd characters modulo d that are trivial on H, so H is balanced.

What can be said about c_χ in general?

If χ is even, then it is almost obvious that $c_\chi = 0$, in fact, that's why the criterion mentions only odd characters.

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 $\chi'(\ell) \neq 1$.

An application: Suppose that $4 \mid d$ and $H = \langle \frac{1}{2}d + 1 \rangle_d$. Note that $\mathbb{U}_d/H \cong \mathbb{U}_{\frac{1}{2}d}$. Thus if χ is a character modulo d that is trivial on H it is essentially a character modulo $\frac{1}{2}d$, so that the conductor d' of χ divides $\frac{1}{2}d$. This shows that d/d' is even, and so the first bullet implies that $c_\chi = 0$. Hence H is balanced.

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 order 4 and order 6. It's possible that a minimal balanced subgroup is always cyclic; so far no counterexamples have been found.

He has also found some infinite families of minimal sporadic subgroups, so maybe the word "sporadic" needs to be replaced...

Despite the existence of such infinite families, P & Ulmer conjecture that for most numbers d for which $\langle p \rangle_d$ is balanced, we have $-1 \in \langle p \rangle_d$ or $4 \mid d$ and $\frac{1}{2}d + 1 \in \langle p \rangle_d$.

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

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

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

Then we conjecture that

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

as $x \to \infty$.

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 $x \to \infty$.

(We show in the case of p an odd prime that we may take $\delta_p = \frac{1}{16}$.)

So the surprise here is 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, $|B_{p,1}(x)| \sim c_p x/(\log x)^{2/3}$.)

Why does this happen?

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

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

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

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

Further, it is an easy exercise to see that when $l_p(m)$ is even that $d \in \mathcal{B}_{p,0}$ if and only if $v_2(l_p(2^j)) > v_2(l_p(m))$.

Further we have $v_2(l_p(2^j)) = j + O_p(1)$.

So, what can we say about $v_2(l_p(m))$? Since m is odd, we have

$$v_2(l_p(m)) = \max\{v_2(l_p(r)) : r \text{ prime}, \ r \mid m\}.$$

We can show that usually $2^{v_2(l_p(m))} \asymp \log\log x$, from which our result then follows.

To anticipate a possible question, I remark that we have sketched 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 $x \to \infty$.

Finally 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 $d \to \infty$, the upper bound implicit here depending on the GRH.

THANK YOU