Erdős-Selfridge and supersingularity

Michael Bennett (joint with Samir Siksek)

University of British Columbia (and Warwick University)

San Diego : January 2018

Products of consecutive integers

Theorem (Erdős - Selfridge, 1975)

The Diophantine equation

$$n(n+1)\cdots(n+k-1) = y^{\ell}$$

has no solutions in positive integers n, k, y *and* ℓ *with* $k, \ell \geq 2$.

Products of consecutive integers

Theorem (Erdős - Selfridge, 1975)

The Diophantine equation

$$n(n+1)\cdots(n+k-1) = y^{\ell}$$

has no solutions in positive integers n, k, y *and* ℓ *with* $k, \ell \geq 2$.

The proof of this result is a combination of clever elementary and graph theoretic arguments.

A Generalization

We will concern ourselves with the Diophantine equation

$$n(n+d)\cdots(n+(k-1)d) = y^{\ell} \qquad (*)$$

where n, d, k, y and ℓ are positive integers with $k, \ell \geq 2$.

A Generalization

We will concern ourselves with the Diophantine equation

$$n(n+d)\cdots(n+(k-1)d) = y^{\ell} \qquad (*)$$

where n, d, k, y and ℓ are positive integers with $k, \ell \geq 2$.

Note that the result of Erdős-Selfridge corresponds to the case $d = 1$. A theorem of Darmon and Merel is a special case of this equation for $k = 3$.

(Necessary) assumptions

In the equation

$$n(n+d)\cdots(n+(k-1)d) = y^{\ell}, \qquad (*)$$

we will assume that $\gcd(n,d) = 1$ and that $(k,\ell) \neq (2,2)$ or $(3,2)$.

(Necessary) assumptions

In the equation

$$n(n+d)\cdots(n+(k-1)d)=y^{\ell}, \qquad (*)$$

we will assume that $\gcd(n,d)=1$ and that $(k,\ell)\neq(2,2)$ or $(3,2)$.

Without these assumptions, we encounter infinitely many solutions, such as

$$9\cdot 18\cdot 27\cdot 36=54^3 \text{ and } 1\cdot 25\cdot 49=35^2.$$

Conjecture (Erdős)

The equation

$$n(n+d)\cdots(n+(k-1)d) = y^{\ell} \qquad (*)$$

has no solutions in relatively prime nonzero integers n, d, k, y *and* ℓ *are positive integers with* $\ell \geq 2$ *and* k *"sufficiently large".*

Prior work

The earliest result on the equation

$$n(n+d)\cdots(n+(k-1)d) = y^{\ell} \qquad (*)$$

is the following.

Theorem (Euler)

The Diophantine equation (*) has no positive solutions with $(k, \ell) = (4, 2)$.

More generally....

One can show that

$$n(n+d)\cdots(n+(k-1)d) = y^{\ell} \qquad (*)$$

has at most finitely many solutions if

More generally....

One can show that

$$n(n+d)\cdots(n+(k-1)d) = y^{\ell} \qquad (*)$$

has at most finitely many solutions if

- d is fixed (Marszalek, 1985)

More generally....

One can show that

$$n(n+d)\cdots(n+(k-1)d) = y^{\ell} \qquad (*)$$

has at most finitely many solutions if

- d is fixed (Marszalek, 1985)
- ℓ and $\omega(d)$ are fixed (Shorey-Tijdeman, 1990)

More generally....

One can show that

$$n(n+d)\cdots(n+(k-1)d) = y^{\ell} \qquad (*)$$

has at most finitely many solutions if

- d is fixed (Marszalek, 1985)
- ℓ and $\omega(d)$ are fixed (Shorey-Tijdeman, 1990)
- ℓ and k are fixed (Darmon-Granville, 1995)

More generally....

One can show that

$$n(n+d)\cdots(n+(k-1)d) = y^{\ell} \qquad (*)$$

has at most finitely many solutions if

- d is fixed (Marszalek, 1985)
- ℓ and $\omega(d)$ are fixed (Shorey-Tijdeman, 1990)
- ℓ and k are fixed (Darmon-Granville, 1995)
- $k \leq 82$ (B-Bruin-Győry-Hajdu, 2006)

More generally....

One can show that

$$n(n+d)\cdots(n+(k-1)d) = y^{\ell} \qquad (*)$$

has at most finitely many solutions if

- d is fixed (Marszalek, 1985)
- ℓ and $\omega(d)$ are fixed (Shorey-Tijdeman, 1990)
- ℓ and k are fixed (Darmon-Granville, 1995)
- $k \leq 82$ (B-Bruin-Győry-Hajdu, 2006)

As noted earlier, Erdős conjectured that (*) has no solutions whatsoever, if k exceeds an absolute constant.

What we can prove

Theorem (B.-Siksek)

There exists an effectively computable absolute constant k_0 such that if $k \geq k_0$, then there are at most finitely many solutions to the equation

$$n(n+d)\cdots(n+(k-1)d) = y^\ell \qquad (*)$$

in nonzero integers n, d, y and ℓ, with $\ell \geq 2$ and $\gcd(n,d) = 1$.

How to proceed

Suppose we have a solution to

$$n(n+d)\cdots(n+(k-1)d) = y^{\ell} \qquad (*)$$

with n and d coprime positive integers. Then we can write

$$n + id = A_i y_i^{\ell} \text{ for each } i = 0, 1, \ldots, k-1,$$

where, in each case, $P(A_i) < k$.

Frey curves

Let $\mathcal{A}$ be the set of (non-trivial) 3-term arithmetic progressions $(i, j, 2j - i)$ in the interval $\{0, 1, \ldots, k - 1\}$; here we always take $j > i$ and thus $2j - i > j$. Associated to any such 3-term arithmetic progression $\mathfrak{a} = (i, j, 2j - i) \in \mathcal{A}$ is a generalized Fermat equation

$$A_i y_i^\ell - 2A_j y_j^\ell + A_{2j-i} y_{2j-i}^\ell = 0\,.$$

To this we associate the Frey curve

$$E_{\mathfrak{a}} \; : \; Y^2 = X(X - A_i y_i^\ell)(X + A_{2j-i} y_{2j-i}^\ell).$$

More Frey curves

For ℓ sufficiently large, $E_{\mathfrak{a}} \sim_\ell F_{\mathfrak{a}}$ where $F_{\mathfrak{a}}/\mathbb{Q}$ has full 2-torsion and conductor $N(F_{\mathfrak{a}})$.

More Frey curves

For ℓ sufficiently large, $E_{\mathfrak{a}} \sim_\ell F_{\mathfrak{a}}$ where $F_{\mathfrak{a}}/\mathbb{Q}$ has full 2-torsion and conductor $N(F_{\mathfrak{a}})$.

What this means is that we have, for all prime $p \nmid 2A_iA_jA_{2j-i}$,

$$a_p(F_{\mathfrak{a}}) \equiv a_p(E_{\mathfrak{a}}) \mod \ell,$$

if, further, $p \nmid y_iy_jy_{2j-i}$, and

$$a_p(F_{\mathfrak{a}}) \equiv \pm(p+1) \mod \ell,$$

if $p \mid y_iy_jy_{2j-i}$. Here $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$.

Primes in $[k/2, k]$

We distinguish between two cases :

Case I : y is divisible by a prime p with $k/2 < p < k$.
Case II : y is not divisible by such a prime.

If we are in the first case, such a p divides exactly one or two of the $n + id$. Suppose the latter, i.e that

$$n + id \quad \text{and } n + (i + p)d \quad \text{are divisible by } p.$$

Without loss of generality (almost!), we may assume that

$$\text{ord}_p(n + (i + p)d) \equiv -1 \bmod \ell.$$

Primes in $[k/2, k]$

Then from the identity

$$(n + (i+1)d) + (p-1)(n + (i+p+1)d) = p(n + (i+p)d),$$

we obtain a ternary equation of the shape

$$Aa^\ell + Bb^\ell = Cc^\ell, \quad \text{where } p \nmid ABCab \text{ and } p \mid c.$$

Primes in $[k/2, k]$

Then from the identity

$$(n + (i+1)d) + (p-1)(n + (i+p+1)d) = p(n + (i+p)d),$$

we obtain a ternary equation of the shape

$$Aa^\ell + Bb^\ell = Cc^\ell, \quad \text{where } p \nmid ABCab \text{ and } p \mid c.$$

For this p, we have $p \leq k$ and

$$a_p(F_{\mathfrak{a}}) \equiv \pm(p+1) \mod \ell.$$

A conclusion

We may thus suppose that, if we have a solution to

$$n(n+d)\cdots(n+(k-1)d) = y^{\ell}, \qquad (*)$$

for suitably large ℓ, then d is necessarily divisible by all primes $k/2 < p < k$.

A conclusion

We may thus suppose that, if we have a solution to

$$n(n+d)\cdots(n+(k-1)d) = y^{\ell}, \qquad (*)$$

for suitably large ℓ, then d is necessarily divisible by all primes $k/2 < p < k$.
Recall, given $\mathfrak{a} = (i, j, 2j-i) \in \mathcal{A}$, we had

$$E_{\mathfrak{a}} \ : \ Y^2 = X(X - A_i y_i^{\ell})(X + A_{2j-i} y_{2j-i}^{\ell}),$$

where $n + id = A_i\, y_i^{\ell}$ and $n + (2j-i)d = A_{2j-i}\, y_{2j-i}^{\ell}$.

A conclusion (continued)

Hence, if $k/2 < p < k$, then $E_{\mathfrak{a}}$ has good reduction at p and is congruent modulo p to the curve

$$\tilde{E} \ : \ Y^2 = X^3 - n^2 X.$$

A conclusion (continued)

Hence, if $k/2 < p < k$, then $E_{\mathfrak{a}}$ has good reduction at p and is congruent modulo p to the curve

$$\tilde{E} \ : \ Y^2 = X^3 - n^2 X.$$

It follows that $a_p(E_{\mathfrak{a}}) = a_p(\tilde{E}) = 0$ for every $k/2 < p < k$ with $p \equiv 3 \mod 4$, i.e. $E_{\mathfrak{a}}$ is supersingular at p.

Supersingular primes

For non-CM curves E, it has been long known (via work of Serre, based upon the Chebotarev density theorem) that if we define

$$\pi_0(k) = \#\{p \leq k : a_p = 0\},$$

then

$$\pi_0(k) = o(\pi(k)) \text{ (even } \pi_0(k) \ll k^{3/4}),$$

while, by construction,

$$\pi_0(k) \gg k/\log(k).$$

The problem lies in the implicit dependence on E.

Towards character sums

Lemma

Let $p \equiv 3 \mod 4$ be prime and suppose that $F/\mathbb{F}_p$ is an elliptic curve of the form

$$F \ : \ Y^2 = X(X-1)(X-\eta^2)$$

for some $\eta \in \mathbb{F}_p \setminus \{0, 1, -1\}$. Then $F(\mathbb{F}_p)$ contains a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

A technical result

Lemma

Let $F/\mathbb{Q}$ be an elliptic curve with full 2-torsion. Let $p \equiv 3 \pmod 8$ be a prime of good supersingular reduction for F. Let $\lambda \in \mathbb{Q}$ be any of the six λ-invariants of F. Then $\mathrm{ord}_p(\lambda) = 0$ and

$$\left(\frac{\lambda}{p}\right) = -1.$$

A technical result

Lemma

Let $F/\mathbb{Q}$ be an elliptic curve with full 2-torsion. Let $p \equiv 3 \pmod 8$ be a prime of good supersingular reduction for F. Let $\lambda \in \mathbb{Q}$ be any of the six λ-invariants of F. Then $\mathrm{ord}_p(\lambda) = 0$ and

$$\left(\frac{\lambda}{p}\right) = -1.$$

Here, F is a quadratic twist of $Y^2 = X(X-1)(X-\lambda)$.

A technical result

Lemma

Let $F/\mathbb{Q}$ be an elliptic curve with full 2-torsion. Let $p \equiv 3 \pmod 8$ be a prime of good supersingular reduction for F. Let $\lambda \in \mathbb{Q}$ be any of the six λ-invariants of F. Then $\mathrm{ord}_p(\lambda) = 0$ and

$$\left(\frac{\lambda}{p}\right) = -1.$$

Here, F is a quadratic twist of $Y^2 = X(X-1)(X-\lambda)$.
Key :

$$\#F(\mathbb{F}_p) = p + 1 \equiv 4 \mod 8.$$

For our purposes, observe that

$$\sum_{\substack{k/2<p\leq k \\ p\equiv 3 \bmod 8}} -\left(\frac{\lambda}{p}\right)\log p \ = \frac{k}{8} + O\left(\frac{k}{\log k}\right)$$

For our purposes, observe that

$$\sum_{\substack{k/2<p\le k\\ p\equiv 3 \bmod 8}} -\left(\frac{\lambda}{p}\right)\log p \;=\frac{k}{8}+O\left(\frac{k}{\log k}\right)$$

Let μ_i be the primitive quadratic Dirichlet characters which on odd primes p away from the support of λ are given by

$$\mu_1(p)=\left(\frac{\lambda}{p}\right),\mu_2(p)=\left(\frac{-\lambda}{p}\right),\mu_3(p)=\left(\frac{2\lambda}{p}\right),\mu_4(p)=\left(\frac{-2\lambda}{p}\right),$$

and observe that

$$\mu_1(p)-\mu_2(p)-\mu_3(p)+\mu_4(p)=\begin{cases}4\left(\frac{\lambda}{p}\right) & \text{if } p\equiv 3 \mod 8\\ 0 & \text{otherwise.}\end{cases}$$

Character sums

Thus

$$\sum_{k/2<p\le k} (-\mu_1(p)+\mu_2(p)+\mu_3(p)-\mu_4(p))\log p \;=\frac{k}{2}+O\left(\frac{k}{\log k}\right)$$

and so for some i, setting $\chi_{\mathfrak{a}}=\mu_i$,

$$\left|\sum_{k/2<m\le k} \chi_{\mathfrak{a}}(m)\Lambda(m)\right| \;>0.124k.$$

The prime number theorem

Theorem

Let χ be a primitive Dirichlet character of conductor N. Then

$$\sum_{m \le X} \chi(m)\Lambda(m) =$$

$$\delta_\chi X - \frac{X^{\beta_\chi}}{\beta_\chi} + O\left(X \exp\left(\frac{-c \log X}{\sqrt{\log X} + \log N}\right) \cdot (\log N)^4\right).$$

Here $\delta_\chi = 0$ unless χ is trivial in which case $\delta_\chi = 1$. Moreover, $c > 0$ is an absolute effective constant, and the implied constant is absolute. Also β_χ denotes the exceptional zero if present, otherwise the term $-X^{\beta_\chi}/\beta_\chi$ is to be omitted.

The prime number theorem

It is worth observing at this point that the "error term" here is actually smaller than the main term (so that the statement in non-trivial), only for suitably small conductor N, relative to the interval of summation X; i.e. only when $\log N \ll \log^{\kappa} X$ for some $\kappa < 1$.

The prime number theorem

It is worth observing at this point that the "error term" here is actually smaller than the main term (so that the statement in non-trivial), only for suitably small conductor N, relative to the interval of summation X; i.e. only when $\log N \ll \log^{\kappa} X$ for some $\kappa < 1$.

We wish to apply this result to characters of conductor roughly $N_{\mathfrak{a}}$, over an interval of length $k/2$.

Smooth numbers

We analyze the various conductors $N_{\mathfrak{a}}$, depending on how *smooth* they are, i.e. we study the relative sizes of $P(N_{\mathfrak{a}})$. We distinguish between $P(N_{\mathfrak{a}})$ *very small*, *small*, *medium* and *large*, depending on whether

$$P(N_{\mathfrak{a}}) < (\log k)^{1-\kappa_1}, \quad \kappa_1 > 0,$$

$$(\log k)^{1-\kappa_1} \leq P(N_{\mathfrak{a}}) \leq 10^4 \log k,$$

$$10^4 \log k < P(N_{\mathfrak{a}}) \leq k^{7/16},$$

and $P(N_{\mathfrak{a}}) \geq k^{7/16}$, respectively.

Brushing details under the rug

Eventually, we are able to show that we have *sufficiently many* $\mathfrak{a}$ with

$$P(N_{\mathfrak{a}}) < (\log k)^{1-\kappa_1}, \quad \kappa_1 > 0,$$

and then, applying an explicit version of the Prime Number Theorem for Dirichlet characters, derive a contradiction.

Brushing details under the rug

Eventually, we are able to show that we have *sufficiently many* $\mathfrak{a}$ with

$$P(N_{\mathfrak{a}}) < (\log k)^{1-\kappa_1}, \quad \kappa_1 > 0,$$

and then, applying an explicit version of the Prime Number Theorem for Dirichlet characters, derive a contradiction.

To get to this stage, we require bounds for character sums in short intervals due to Iwaniec and to Graham and Ringrose, the large sieve of Bombieri, the theorems of Roth and of Varnavides on 3-term arithmetic progressions in thin sets and computational data of Platt on zeros of Dirichlet L-functions.