Small gaps between primes (after Goldston-Pintz-Yıldırım)

In this section, we introduce the strategy initiated by Goldston-Yıldırım, and carried out by them and Pintz, for proving new results on the existence of short gaps between primes. Some calculations are postponed to a later unit.

References: much of this unit is liberally plagiarized from K. Soundararajan, Small gaps between prime numbers: the work of Goldston-Pintz-Yıldırım, *Bull. Amer. Math. Soc.* **44** (2007), 1–18. For more details (which will be plagiarized later), see D.A. Goldston, Y. Motodashi, J. Pintz, and C. Yıldırım, Small gaps between primes exist, *Proc. Japan Acad. Ser. A Math. Sci.* **82** (2006), 61–65. (Both references are available online, e.g., via MathSciNet.)

1 The target theorem

Let p_n denote the n-th prime. As noted in the previous unit, we can use a probabilistic model to make plausible predictions about the ratio $(p_{n+1} - p_n)/(\log p_n)$, by supposing that $\pi(x + y) - \pi(x)$, for x large and $y \sim \lambda \log x$, obeys a Poisson distribution with parameter λ.

What we will prove is a rather crude assertion consistent with this model. (Before this work, this was only known for $\epsilon \approx 0.24$.)

Theorem 1 (GPY). *For any $\epsilon > 0$, there exist infinitely many p_n such that $p_{n+1} - p_n < \epsilon \log p_n$.*

Goldston et al also get a quantitative version of this, and they can even do this with $p_{n+1} - p_n < (\log p_n)^{1-\epsilon}$ for some specific $\epsilon > 0$. For simplicity, I won't get into these improvements. But I will discuss the following, whose proof is a good setup for the proof of Theorem 1.

Theorem 2 (GPY). *Assume the Elliott-Halberstam conjecture for $Q = x^\theta$ with any fixed $\theta > 1/2$. Then there exists $c = c(\theta)$ such that there exist infinitely many p_n such that $p_{n+1} - p_n < c$. (If $\theta > 20/21$, one has $c(\theta) = 20$.)*

2 The approach

Fix a positive integer k; the basic idea is to try to prove a weak version of the Hardy-Littlewood k-tuples conjecture, for a k-tuple $\mathcal{H} = (h_1, \ldots, h_k)$ of distinct integers. Namely, we'll try to prove that there are infinitely many n such that *at least two* of $n + h_1, \ldots, n + h_k$ are prime; this would imply that there are infinitely many prime gaps no greater than $\max \mathcal{H} - \min \mathcal{H}$.

To do this, we will try to find an arithmetic function $a(n)$ with nonnegative values, such that for $j = 1, \ldots, k$, we can establish

$$\sum_{x < n \le 2x, n+h_j = p} a(n) > \frac{1}{k} \sum_{x < n \le 2x} a(n). \tag{1}$$

If we had such a function, we could sum over j to obtain

$$\sum_{x<n\leq 2x} \#\{1 \leq j \leq k : n + h_j \text{ prime}\} \cdot a(n) > \sum_{x<n\leq 2x} a(n),$$

which would immediately imply that for some $x < n \leq 2x$, at least two of $n + h_1, \ldots, n + h_k$ are prime. (Note: this strategy is poorly adapted to look for three or more primes in the same tuple. In fact, no satisfactory alternative has been proposed!)

Note that if $a(n)$ is supported only on those n for which $n + h_1, \ldots, n + h_k$ is prime, then the k-tuples conjecture would imply (1), but we have no hope of proving (1) directly. Instead, we make a transition that is directly inspired by the transition from the combinatorial sieve to the Selberg sieve.

3   Selberg revisited

Namely, we pick a cutoff parameter R (which will ultimately depend on k and x), and choose $a(n)$ of the form

$$a(n) = \left(\sum_{d|(n+h_1)\cdots(n+h_k)} \rho(d) \right)^2$$

for some arithmetic function ρ with $\rho(1) = 1$ and support in $\{1, \ldots, R\}$. As in Selberg's sieve, we have built the nonnegativity requirement into the construction, and we are now free to vary the values of ρ in order to maximize the ratio between the two sides of (1).

Unfortunately, we are not in as simple a situation as in Selberg's sieve, where we could simply diagonalize a quadratic form to find the desired minimum. In our case, we are comparing two different quadratic forms, which cannot be simultaneously diagonalized, and hitting the situation with Lagrange multipliers creates a mess. The best we can hope to do is to pick ρ of a special form with at least one parameter left in, run the calculation, and then optimize the choice of the parameter(s).

In Selberg's sieve, the optimal choice would have been

$$\rho(d) \approx \mu(d) \left(\frac{\log R/d}{\log R} \right)^k \qquad (d \leq R).$$

In our setting, we will instead put

$$\rho(d) = \mu(d) \left(\frac{\log R/d}{\log R} \right)^{k+\ell} \qquad (d \leq R) \tag{2}$$

for ℓ a nonnegative integer depending on k, in a fashion to be specified later.

2

4   Comparing the two sides

With this choice, one can calculate the two sides of (1) using the sorts of techniques we used in the first section of this course. I will postpone those calculations to a later unit, so that I can continue giving an overview of the method. First, here is what one gets for the right side of (1).

Lemma 3. *With notation as above, there exist $C, c > 0$ depending on k, ℓ, such that for $R \leq x^{1/2}/(\log x)^C$,*

$$\sum_{x < n \leq 2x} a(n) = \frac{\mathfrak{S}(\mathcal{H})(k+\ell)!^2}{(k+2\ell)!(\log R)^{2k+2\ell}} \binom{2\ell}{\ell} x (\log R)^{k+2\ell} + O\left(\frac{x(\log x)^{k+2\ell-1}(\log\log x)^c}{(\log R)^{2k+2\ell}}\right).$$

The left side of (1) is more complicated, because of the extra restriction that $n + h_j$ must be prime. It is on this side that the arithmetic subtleties will creep in. Expanding the square, we get

$$\sum_{d_1, d_2 \leq R} \rho(d_1)\rho(d_2) \#\{x < n \leq 2x : [d_1, d_2] | (n + h_1) \cdots (n + h_k), n + h_j \text{ prime}\}. \qquad (3)$$

The count on the right side involves first pinning n down among some number of arithmetic progressions modulo the lcm $[d_1, d_2]$, then looking for primes in that arithmetic progression. Thus one expects to be able to approximate (3) by

$$\frac{x}{\log x} \sum_{d_1, d_2 \leq R} \rho(d_1)\rho(d_2) \frac{g([d_1, d_2])}{\phi([d_1, d_2])}, \qquad (4)$$

where g is the multiplicative function with $g(p) = v_{\mathcal{H}}(p) - 1$.

Lemma 4. *With notation as above, there exist $C, c > 0$ depending on k, ℓ, such that for $R \leq x^{1/2}/(\log x)^C$, we have the following.*

(a) For $h \notin \mathcal{H}$, (4) equals

$$\frac{\mathfrak{S}(\mathcal{H}, h)}{(\log R)^{2k+2\ell}} \frac{(k+\ell)!^2}{(k+2\ell)!} \binom{2\ell}{\ell} \frac{x}{\log x} (\log R)^{k+2\ell} + O\left(\frac{x(\log x)^{k+2\ell-2}(\log\log x)^c}{(\log R)^{2k+2\ell}}\right).$$

(b) For $h \in \mathcal{H}$, (4) equals

$$\frac{\mathfrak{S}(\mathcal{H})}{(\log R)^{2k+2\ell}} \frac{(k+\ell)!^2}{(k+2\ell+1)!} \binom{2(\ell+1)}{\ell+1} \frac{x}{\log x} (\log R)^{k+2\ell+1} + O\left(\frac{x(\log x)^{k+2\ell-1}(\log\log x)^c}{(\log R)^{2k+2\ell}}\right).$$

Crunching the numbers, we see that the ratio between (4) and the right side of (1) is asymptotic to

$$\frac{\log R}{\log x} \frac{2k(2\ell+1)}{(\ell+1)(k+2\ell+1)}. \qquad (5)$$

3

The second fraction is always less than 4, but it tends to 4 as $k, \ell \to \infty$. Thus if we can safely approximate (3) by (4) in the range $R \leq x^{1/2-\epsilon}$, or even $R \leq x^{1/4+\epsilon}$, we get bounded gaps between primes. (Here's where we get stuck looking for three primes in one tuple: we can't hope to get past $R = x^{1/2-\epsilon}$ because of our earlier errors.) For instance, if we could take $R = x^{1/2-\epsilon}$, then already we get (4) with $k = 7, \ell = 1$. Using the 7-tuple $\mathcal{H} = \{11, 13, 17, 19, 23, 29, 31\}$, one then deduces that there are infinitely many prime gaps of size at most 20.

One can tweak the above argument by changing (2) to allow a polynomial $P(\log(R/d)/(\log R))$ instead of just a power. That polynomial must satisfy $P(1) = 1$ and must vanish to order at least k at 0. The quantity analogous to (5) is

$$\frac{\log R}{\log x} k \frac{\int_0^1 \frac{y^{k-2}}{(k-2)!} P^{(k-1)}(1-y)^2 \, dy}{\int_0^1 \frac{y^{k-1}}{(k-1)!} P^{(k)}(1-y)^2 \, dy}. \tag{6}$$

If we can take $R = x^{1/2-\epsilon}$, then one can get this ratio over 1 already with $k = 6$, so one gets infinitely many prime gaps bounded by 16 (using $\mathcal{H} = \{7, 11, 13, 17, 19, 23\}$) rather than 20. But even with the flexibility of choosing P, one can never get the second factor (excluding $(\log R)/(\log x)$) over 4 (exercise)!

5 The error terms, first attempt

None of the above matters unless we can control the discrepancy between (3) and (4). This discrepancy is spawned by error terms in the prime number theorem with moduli of the form $[d_1, d_2]$ for $d_1, d_2 \leq R$, so the moduli can run up to R^2.

Now recall what we know about these discrepancies. Let $\pi(x; N, m)$ be the number of primes $p \leq x$ congruent to m modulo N. If we allow Elliott-Halberstam, then for any fixed $A > 0$ and $\epsilon > 0$, there exists $c > 0$ such that

$$\sum_{q \leq Q} \max_{m \in (\mathbb{Z}/N\mathbb{Z})^*} \left| \pi(2x; N, m) - \pi(x; N, m) - \frac{x}{\phi(N) \log x} \right| \leq cx(\log x)^{-A}$$

for $Q = x^{1-\epsilon}$. This would allow taking $R = x^{1/2-\epsilon}$; we thus deduce Theorem 2.

Unconditionally, Bombieri-Vinogradov only allows $Q = x^{1/2-\epsilon}$. This looks like a disaster: we must take $R = x^{1/4-\epsilon}$, and so we can never get (1)! What now?

6 The error terms, second attempt

Remember that Theorem 1 is a much weaker assertion than the existence of infinitely many bounded gaps between primes; there is thus no need to insist on establishing (1) for any particular tuple $\mathcal{H}$. Instead, we are free to aggregate over all $\mathcal{H}$ in a certain range; to clarify, write $a(n; \mathcal{H})$ instead of $a(n)$ to indicate the dependence on $\mathcal{H}$.

Fix $\delta > 0$ for which we want infinitely many n with $p_{n+1} - p_n \leq H = \delta \log x$. We will now try to prove the inequality

$$\sum_{\mathcal{H} \in \{1,\ldots,H\}^k} \sum_{1 \leq h \leq H, n+h=p} a(n, \mathcal{H}, h) > \frac{1}{h} \sum_{\mathcal{H} \in \{1,\ldots,H\}^k} \sum_{1 \leq h \leq H, n+h=p} \sum_{x < n \leq 2x} a(n, \mathcal{H}), \qquad (7)$$

which again is enough: now we get an n such that at least two of $n+1, \ldots, n+h$ are prime.

For the right side of (7), Gallagher's result from the previous unit gives us the same asymptotics as before, except with $\mathfrak{S}(\mathcal{H})$ replaced by 1 and slightly worse error terms. We get an improvement on the left side, which we separate into terms with $h \notin \mathcal{H}$ and terms with $h \in \mathcal{H}$. We estimate the latter termse exactly as before; for the former terms, we note that if $n + h$ is prime, then

$$a(n; \mathcal{H}) = a(n; \mathcal{H}, h).$$

Namely, the difference comes from summands d which divide $(n+h_1)\cdots(n+h_k)(n+h)$ but not $(n+h_1)\cdots(n+h_k)$; those are all multiples of $n + h > x > R$, so $\rho(d) = 0$ for such d.

Thus we can simply appeal back to Lemma 3 with k replaced by $k+1$ and $\mathcal{H}$ replaced by $\mathcal{H}, h$. If we now compare the ratio of the two sides of (7), the contribution in the numerator from $h \in \mathcal{H}$ is exactly (5), to which we add the contribution $H/(\log x) = \delta$ from the terms with $h \notin \mathcal{H}$. As noted earlier, that's just enough to get over 1 with $R = x^{1/2-\epsilon}$ and k, ℓ sufficiently large. This yields Theorem 1.

Exercises

1. Use the Poisson distribution model to compute a predicted distribution for the ratio $(p_{n+1} - p_n)/(\log p_n)$.

2. Say we want to produce *large* gaps between primes. Take N to be the product of the primes up to m, and consider $N + 2, \ldots, N + m$. For what function f does this imply $p_{n+1} - p_n > f(p_n)$ for infinitely many n?

3. Let P be a polynomial with $P(1) = 1$ vanishing to order at least k at 0. Prove that the quantity (6) sans the factor $(\log R)/(\log x)$ is at most 4.