PRIMES IN ARITHMETIC PROGRESSIONS: FIXED MODULUS
COURSE NOTES, 2015

In this section, we survey the theory of primes in arithmetic progressions $p = a \mod q$, $p \leq x$, with the modulus q being fixed and $x \to \infty$.

1. Elementary cases of Dirichlet's theorem

Dirichlet's theorem says that if $\gcd(a, q) = 1$ then there are infinitely many primes in the progression $p = a \mod q$. The proof is the subject of a separate course, though some in the class have seen it (possibly in $\mathbb{F}_q[t]$). Instead, we explain some elementary examples.

1.1. $p = 3 \mod 4$. Assume there are only finitely many primes $p = 3 \mod 4$. Enumerate them as $p_1 = 3, p_2 = 7, \dots, p_M$. Let

$$N := 4p_1 \cdots \cdot p_M - 1$$

Then $N > 1$, $2 \nmid N$, and $p_j \nmid N$, hence all prime factors of N are congruent to $1 \mod 4$: $N = q_1 \dots q_r$, $q_j = 1 \mod 4$. But then $N = 1 \mod 4$, contradiction.

1.2. $p = 1 \mod 4$. Assume that there are only finitely many primes $p = 1 \mod 4$. Enumerate them as $p_1 = 5, p_2 = 13, \dots, p_M$. Let

$$N = (2p_1 \dots p_M)^2 + 1$$

Then $N > 1$, $2 \nmid N$, $p_j \nmid N$ and hence all prime factors of N are $= 3 \mod 4$. Since $N > 1$. there is at least one such prime $p \mid N$. Then

$$(2p_1 \dots p_M)^2 = -1 \mod p$$

But since $p = 3 \mod 4$, we know that $-1 \neq \square \mod p$ hence we have a contradiction.

1.3. $p = 1 \mod q$, $q > 2$ prime. We take an odd prime q and show there are infinitely many primes $p = 1 \mod q$. Otherwise, list them as $p_1, \dots, p_M$ (possibly there are none).

Let

$$\Phi_q(x) = 1 + x + \dots + x^{q-1} = \frac{x^q - 1}{x - 1}$$

be the cyclotomic polynomial. Let

$$A := q \cdot \prod_{j=1}^{M} p_j$$

Date: May 26, 2015.

$$N := \Phi_q(A) = 1 + A + \cdots + A^{q-1} = \frac{A^q - 1}{A - 1}$$

Then $N > 1$, $q \nmid N$, $p_j \nmid N$.

Since $N > 1$, there is some prime p dividing N. Then

$$A^q = 1 \mod p$$

and hence either $A = 1 \mod p$ or $\mathrm{ord}_p(A) = q$. In the latter case, this implies that $q = \mathrm{ord}_p(A) \mid p - 1$ so that $p = 1 \mod q$, contradiction.

We rule out $A = 1 \mod p$, since otherwise we find

$$N = 1 + A + \cdots + A^{q-1} = 1 + \ldots 1 = q \mod p$$

and since $p \mid N$, also $N = 0 \mod p$, hence $q = 0 \mod p$. Since both p and q are prime, this forces $p = q$. But we saw $q \nmid N$, contradiction.

2. The PNT for arithmetic progressions

Let $\gcd(a, q) = 1$, and set

$$\pi(x; q, a) := \#\{p \le x : p = a \mod q\}$$

$$\theta(x; q, a) := \sum_{\substack{p \le x \\ p = a \mod q}} \log p$$

(the sum over primes),

$$\psi(x; q, a) := \sum_{\substack{n \le x \\ n = a \mod q}} \Lambda(n)$$

The prime number theorem for arithmetic progressions states that if $\gcd(a, q) = 1$, then as $x \to \infty$ (q fixed),

$$\pi(x; q, a) = \frac{1}{\phi(q)} \mathrm{Li}(x) + O(xe^{-c\sqrt{\log x}})$$

$$\psi(x; q, a) = \frac{x}{\phi(q)} + O(xe^{-c\sqrt{\log x}})$$

Applying summation by parts gives

$$\sum_{\substack{p \le x \\ p = a \mod q}} \frac{\log p}{p} = \frac{1}{\phi(q)} \log x + O(1) \tag{1}$$

Exercise: prove this.

Recall that we take q fixed, and $x \to \infty$. Later on we will come to the more interesting and important case of varying modulus.

2.1. **Bounding prime values of n^2+1.** It is an old conjecture that there are infinitely many primes of the form n^2+1. In this section we shall give an upper bound for their number

Theorem 2.1. *The number of $n \le x$ so that n^2+1 is prime is $\ll x/\log x$.*

We wish to use the Selberg upper bound sieve, with the sequence

$$\mathcal{A} = \{n^2+1 : n \le x\}$$

If a prime p divides an integer of the form n^2+1, then $p \ne 3 \mod 4$. Hence we take as the set of primes

$$\mathcal{P} = \{p : p \ne 3 \mod 4\}$$

and set

$$P(z) = \prod_{p \le z} p$$

If $d \mid P(z)$, then as we have already seen elsewhere,

$$\#\mathcal{A}_d := \#\{n \le x : d \nmid n^2+1\} = \frac{\rho(d)}{d}x + O(\rho(d))$$

where $\rho(d) = \#\{c \mod d : c^2+1 = 0 \mod d\}$.

Setting

$$\mathcal{S}(\mathcal{A},\mathcal{P},z) := \#\{a \in \mathcal{A} : \gcd(a, P(z)) = 1\}$$

then clearly $\#\mathcal{S}(\mathcal{A},\mathcal{P},z)$ gives an upper bound for the primes $p > z$ of the form n^2+1.

By the Selberg upper bound sieve,

$$\#\mathcal{S}(\mathcal{A},\mathcal{P},z) \le \frac{x}{S(z)} + R(z)$$

where

$$R(z) = \sum_{\substack{d_1,d_2 \le z \\ d \mid P(z)}} \rho([d_1,d_2])$$

and

$$S(z) = \sum_{\substack{d \le z \\ d \mid P(z)}} \frac{1}{f * \mu(d)}$$

where for $d \mid P(z)$, we set $f(d) = d/\rho(d)$.

Theorem 2.2. *Let $\rho(p)$ be as above. Suppose in addition that*

$$\sum_{p \le z} \frac{\omega(p)\log p}{p} = \kappa \log z + O(1),$$

for some $\kappa \ge 0$. Then

$$S(z) \asymp (\log z)^{\kappa}.$$

In our case, $\kappa = 1$: Indeed, if $p = 1 \mod 4$ then $\rho(p) = 2$ while $\rho(p) = 0$ for $p = 3 \mod 4$. Hence

$$\sum_{p \le z} \frac{\rho(p) \log p}{p} = \sum_{\substack{p \le z \\ p = 1 \mod 4}} 2 \frac{\log p}{p} + O(1)$$

and since

$$\sum_{\substack{p \le z \\ p = a \mod q}} \frac{\log p}{p} = \frac{1}{\phi(q)} \log z + O(1)$$

whenever $\gcd(a, q) = 1$, takeing $q = 4$, $a = 1$ gives

$$\sum_{\substack{p \le z \\ p = 1 \mod 4}} \frac{\log p}{p} = \frac{1}{2} \log z + O(1)$$

Thus we find that $S(z) \asymp \log z$.

As for the remainder term $R(z)$, we use for $d_1, d_2 \mid P(z)$, so are squarefree, that

$$\rho([d_1, d_2]) = \prod_{p \mid [d_1, d_2]} \rho(p) \le \rho(d_1) \cdot \rho(d_2)$$

and hence

$$R(z) \le \sum_{\substack{d_1, d_2 \le z \\ d_1, d_2 \mid P(z)}} \rho(d_1) \rho(d_2) = \Big(\sum_{\substack{d \le z \\ d \mid P(z)}} \rho(d) \Big)^2$$

Now for d squarefree,

$$\rho(d) = \prod_{p \mid d} \rho(p) \le \prod_{p \mid d} 2 = \tau(d)$$

(τ is the divisor function), and therefgore

$$\sum_{\substack{d \le z \\ d \mid P(z)}} \rho(d) \le \sum_{d \le z} \tau(d) \sim z \log z$$

Thus we find

$$R(z) \ll z^2 (\log z)^2$$

Altogether we obtain

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, z) \ll \frac{x}{\log z} + z^2 (\log z)^2 \ll \frac{x}{\log x}$$

on taking say $z = x^{1/3}$.