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 \( p_1 = 3, p_2 = 7, \ldots, p_M \). Let

\[
N := 4p_1 \cdots p_M - 1
\]

Then \( N > 1, 2 \nmid N \), and \( p_j \nmid N \), hence all prime factors of \( N \) are congruent to 1 mod 4: \( N = q_1 \cdots q_r, q_j = 1 \mod 4 \). 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 \( p_1 = 5, p_2 = 13, \ldots, p_M \). Let

\[
N = (2p_1 \cdots p_M)^2 + 1
\]

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

\[
(2p_1 \cdots p_M)^2 = -1 \mod p
\]

But since \( p = 3 \mod 4 \), we know that \(-1 \not\equiv \square \mod p\) 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 \( p_1, \ldots, p_M \) (possibly there are none).

Let

\[
\Phi_q(x) = 1 + x + \cdots + x^{q-1} = \frac{x^q - 1}{x - 1}
\]

be the cyclotomic polynomial. Let

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

Date: May 26, 2015.
2 PRIMES IN ARITHMETIC PROGRESSIONS: FIXED MODULUS

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

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 \( \text{ord}_p(A) = q \). In the latter case, this implies that \( q = \text{ord}_p(A) \mid p - 1 \) so that \( p = 1 \mod q \), contradiction.

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

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

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

\[ \pi(x; q, a) := \# \{ p \leq x : p = a \mod q \} \]

\[ \theta(x; q, a) := \sum_{\substack{p \leq x \\ AT\ 0 \ mod\ q}} \log p \]

(the sum over primes),

\[ \psi(x; q, a) := \sum_{n \leq x \mod q} \Lambda(n) \]

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

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

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

Applying summation by parts gives

\[ \sum_{\substack{p \leq x \\ AT\ 0 \ mod\ q}} \frac{\log p}{p} = \frac{1}{\phi(q)} \log x + O(1) \]

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 \( n \leq x \) so that \( n^2 + 1 \) is prime is \( \ll x / \log x \).

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

\[ A = \{ n^2 + 1 : n \leq x \} \]

If a prime \( p \) divides an integer of the form \( n^2 + 1 \), then \( p \not\equiv 3 \mod 4 \). Hence we take as the set of primes

\[ P = \{ p : p \neq 3 \mod 4 \} \]

and set

\[ P(z) = \prod_{p \leq z} p \]

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

\[ \#A_d := \# \{ n \leq x : d \nmid n^2 + 1 \} = \frac{\rho(d)}{d} x + O(\rho(d)) \]

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

Setting

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

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

By the Selberg upper bound sieve,

\[ \#S(A, P, z) \leq \frac{x}{S(z)} + R(z) \]

where

\[ R(z) = \sum_{d, d_2 \leq z \atop d \mid P(z)} \frac{\rho([d_1, d_2])}{d} \]

and

\[ S(z) = \sum_{d \leq z \atop d \mid P(z)} \frac{1}{f \ast \mu(d)} \]

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

\[ \sum_{p \leq z} \frac{\omega(p) \log p}{p} = \kappa \log z + O(1) \]

for some \( \kappa \geq 0 \). Then

\[ S(z) \sim (\log z)^\kappa. \]
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

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

and since

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

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

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

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

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

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

and hence

$$R(z) \leq \sum_{d_1, d_2 \leq z, \ d_1, d_2 | P(z)} \rho(d_1) \rho(d_2) = \left( \sum_{d \leq z, d | P(z)} \rho(d) \right)^2$$

Now for $d$ squarefree,

$$\rho(d) = \prod_{p | d} \rho(p) \leq \prod_{p | d} 2 = \tau(d)$$

($\tau$ is the divisor function), and therefore

$$\sum_{d \leq z, d | P(z)} \rho(d) \leq \sum_{d \leq z} \tau(d) \sim z \log z$$

Thus we find

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

Altogether we obtain

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

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