M823 Introduction to Analytic Number Theory Notes

Ryan May

18/10/2018

Chapter 1

infinite number of primes Tp prove that we have an infinite number of primes let $N = p_1 p_2 ... p_n$ be a composite of all the prime numbers. With $N+1$ this is either a prime, or a composite of primes. It cannot be a prime as $N+1 > p_n$ so it must be composite. As a composite then $p|N$ for some $p > 1$, but also $p|N+1$, so we are saying that $p|1$ which is impossible, and therefore $N+1$ must be prime, proving that there are an infinite number of primes.

infinite number of primes of 4k-1 Let $N = 4p_1 p_2 .. p_n - 1$ where $p_1 p_2 ... p_n$ are all the primes. As $N > p_n$ it is therefore a composite with an odd prime divisor. Let $p|N$ where p is an odd prime divisor we have $p|4N-1$, but then $p|1$ which is impossible. Therefore p cannot be a prime divisor in the form $4k-1$, so all primes must be in the form $4N+1$, but $(4a+1)(4b+1) = 16ab+4a+4b+1 = 4(4ab+a+b)+1 = 4c+1$ which means that N must also be in this form. As it is not, then we have a contradiction thus there are infinite number of primes of $4k-1$.

Using the Euclidean Algorithm to determine gcd For example, finding $\gcd(231, 161)$:

$$\begin{aligned} 231 &= (1)161 + 70 \\ 161 &= (2)70 + 21 \\ 70 &= (3)21 + 7 \\ 21 &= (3)7 + 0 \end{aligned}$$

Thus the $\gcd(231, 161)$ is 7

Using the Euclidean Algorithm backwards Solve First divide both sides by 5 to get $73x + 51y = 1$ Then carry out the Eulidean Algorithm

$$\begin{aligned} 73 &= (1)51 + 22 \\ 51 &= (2)22 + 7 \\ 22 &= (3)7 + 1 \\ 7 &= (7)1 + 0 \end{aligned}$$

Rearrange to give:

$$\begin{aligned} 22 &= 73 + (-1)51 \\ 7 &= 51 + (-2)22 + 7 \\ 1 &= 22 + (-3)7 \end{aligned}$$

Then solve for 1

$$\begin{aligned}
1 &= 22 + (-3)7 \\
&= 22 + (-3)(51 + (-2)22) \\
&= 22 + (-3)51 + (6)22) \\
&= (-3)51 + (7)22) \\
&= (-3)51 + (7)(73 + (-1)51) \\
&= (-3)51 + (7)73 + (-7)51) \\
&= (-10)51 + (7)73
\end{aligned}$$

thus $x = 7$ and $y = -10$

11 For equations with more than two unknowns then remember that $gcd(a, b, c) = gcd((a, b)c)$ Thus work out $gcd(a, b)$, then once you have the last remainder > 0, say r, workout $gcd(c, r)$ To make things easier, if you find a common divisor, divide all sides by that first e.g $55x + 60y = 15$ can be divided by 5 to give $11x + 12y = 5$. Once worked out note that $480 \cdot 225 - 225 \cdot 480 = 0$. Since gcd(225, 480) = 15, you can divide this all by 15 to get

$$32 \cdot 225 - 15 \cdot 480 = 0$$

.

Using $225s + 480t = 15$ working out gives $s = 15$, $t = -7$ So, you can add a multiple of 32 to s and subtract the same multiple of 15 from t. For example, $s = 47$, $t = -22$ is another solution.

Chapter 2

$$f \circ g = f(g(x))$$

Dirichlet Convolution For functions f and g, the function $*$ is defined as: $h = f * g$ is the dirichlet product where

$$(f * g)(n) = \sum f(n)g(\frac{n}{d})$$

It's important to distinguish between a function and an evaluation of a function at a particular integer. E.g. f is a function, $f(n)$ is an evaluation of f at the integer n. this is important because the Dirichlet convolution acts on functions, not their evaluations. i.e. $f(n) * g(n)$ makes no sense. Note that $f * g$ is a function and is defined by its evaluation at each interger, namely $(f * g](n)$.

$(f * g) * h = f * (g * h)$ proof:

$$\begin{aligned}
[(f * g) * h](n) &= \sum_{d|n} (f * g)(d) h\left(\frac{n}{d}\right) \\
&= \sum_{d|n} \sum_{q|d} f(q) g\left(\frac{d}{q}\right) h\left(\frac{n}{d}\right) \\
[f * (g * h)](n) &= \sum_{d|n} f(d)(g * h)\left(\frac{n}{d}\right) \\
&= \sum_{d|n} \sum_{q|n/d} f(d) g(q) h\left(\frac{n}{qd}\right)
\end{aligned}$$

for $n = 6$ $d = \{1, 2, 3, 6\}$

d	1	2	2	3	3	6	6	6	6
q	1	1	2	1	3	1	2	3	6
n/d	6	3		2		1			
d/q	....								

Number theoretic function F

$$f(n) = \sum_{d|n} f(d)$$

Identity function

$$I(n) = \left[\frac{1}{n}\right] = \begin{cases} 1, & \text{if } n = 1. \\ 0, & \text{if } n > 1. \end{cases}$$

Proof:

$$(f * I)(n) = \sum_{d|n} f(d)I(n/d)$$

With $I(n/d) = 0$ for all except when $n = d$, giving $I(1) = 1$. Substituting the above equation for $d = n$

$$\sum_{d|n} f(n)I(n/n) = \sum_{d|n} f(n)I(1) = f(n)$$

likewise:

$$(I * f)(n) = \sum_{d|n} I(d)f(n/d)$$

With $I(d) = 0$ for all except when $d = 1$

$$\sum_{d|n} I(1)f(n/1) = f(n)$$

An example of the proof is when $n = 6$

$$(f * g)(6) = \sum_{d|6} f(d)I(6/d) = f(1)g(6) + f(2)g(3) + f(3)g(2) + f(6)g(1)$$

For $g = I$, $I = 0$ for all except when $f(6)g(1) = f(6)(1) = f(6) = f(n)$

The Mobius Function

$$\mu(1) = 1;$$

If $n > 1$ then write $n = p_1^{a_1}...p_k^{a_k}$. Then

$$\mu(n) = (-1)^k if a_1 = a_2 = a_k = 1$$
$$\mu(n) = 0 \text{ otherwise}$$

For example:

$$\mu(10) = 5 \times 2 = (-1)^2 = 1$$
$$\mu(4) = 2 \times 2 = 2^2 = 0$$

If $n \geq 1$ we have:

$$\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1, & \text{if } n = 1. \\ 0, & \text{if } n > 1. \end{cases}$$

The Euler Totient Function If $n \geq 1$ then $\varphi(n)$ is defined to be the number of positive integers not exceeding n which are relatively prime to n

$$\varphi(n) = \sum_{k=1}^{n}{}' 1$$

where the ' indicates that the sum is extended over those k relatively prime to n
For example:

$$\begin{aligned}
\varphi(3) &= \{1, 2\} = 2 \\
\varphi(4) &= \{1, 3\} = 2 \\
\varphi(5) &= \{1, 2, 3, 4\} = 4 \\
\varphi(p) &= p - 1
\end{aligned}$$

As with the above there is a simple divisor sum

$$\varphi(n) = \sum_{d|n} \varphi(d)$$

For $n \geq 1$

$$\sum_{d|n} \varphi(d) = n$$

$$\sum_{n \leq x} \varphi(n) = \varphi(1) + \varphi(2) + ... + \varphi(x)$$

Example: Determine all the integers n for which $\phi(n) = 16$

Fist of all find all the divisors of 16, that is $d = 1, 2, 4, 8, 16$ now either $p_1^{k_1} p_2^{k_2} ... p_n^{k_n} | 16$ or $p - 1 | 16$ With $\phi(n) = 16 = 2^4$ and $p - 1 | 16$ checking each $d + 1 = p$ we have $n = 2^a 3^b 5^c 17^d$

Working systematically:

If $17|n$, so that $d = 1$ as $d > 1$ gives $\phi(17^2) = 17^2 - 17 > 16$. so $\phi(n) = \phi(17)\phi(m) = 16\phi(m)$ giving $\phi(m) = 1$. Thus $m = 1$ or 2. So we have

$$n = 17 \text{ and } n = 34$$

Now assume that $d = 0$ we have 5^c, Using theorem 2.5a $\phi(5^2) = 5^2 - 5 = 20 > 16$ so we have $c = 1$ $\phi(n) = \phi(5)\phi(m) = 4\phi(m)$ so $\phi(n) = 4\phi(\cdot 2^a 3^b) = 16$, therefore $\phi(2^a 3^b) = 4$.

$3^2 = 3^2 - 3 > 4$ so $b \leq 1$. $\phi(3) = 2$ so we have $\phi(5 \cdot 3 \cdot m) = 4 \cdot 2\phi(m)$ so $\phi(m) = 2$. $\phi(2^2) = 2^2 - 2 = 2$, thus we have the answer

$$n = 5 \cdot 3 \cdot 2^2 = 60$$

Exhausting $b = 1$, setting $b = 0$ we have $\phi(5 \cdot m) = 4\phi(2^a) = 16$. $\phi(2^3) = 2^3 - 2^2 = 4$, so $\phi(n) = \phi(2^3)\phi(5) = 16\phi(m)$, thus

$$n = 5 \cdot 2^3 \cdot 1 = 40$$

So now we have c, $3^3 - 3^2 > 16$ so we have $c \leq 2$ With $c = 2$ $\phi(3^2) = 6$ so $n = 6\phi(m)$ as $6 \not| 16$ then this is impossible. so $c \leq 1$. $\phi(3) = 2$ so $\phi(n) = 2\phi(m) = 16$ giving $\phi(m) = 8$. This is $\phi(m) = \phi(2^4) = 8$ thus we have

$$n = 3 \cdot 2^4 = 48$$

Lastly, with $b = 0$ we have $\phi(2^5) = 16$ giving $n = 32$

Thus

$$n = \{17, 32, 34, 40, 48, 60\}$$

other functions we have:
$\mathbf{u(n)} = \mathbf{1}$, for all n. Known as the **unit function**;
$\sigma_(n) =$ the number of divisors of n — for example, $\sigma_0(6) = 4$;
$\sigma_1(n) =$ the sum of the divisors of n — for example, $\sigma_1(6) = 12$.
The functions $\sigma_0(n)$ and $\sigma_1(n)$ are often called $d(n)$ or $\tau(n)$, and $\sigma(n)$, respectively
$f_\alpha(n) = n^\alpha$, $f_\alpha = N^\alpha$ known as the **power function**.

$$(\mu * u)(n) = \sum \mu(d) = I(n)$$

$$(u * u)(n) = \sum 1 = \sigma_0(n)$$

$$(N * u)(n) = \sum d = \sigma_1(n)$$

Examples:
Prove that

$$\sum_{d|n} \sigma_5(d) = n^5 \sum_{d|n} \sigma_5(d)/d^5$$

$$\begin{aligned}\sum_{d|n}\sigma_5(d) &= \sum_{d|n}\sigma_5(d)\cdot 1\\ &= \sum_{d|n}\sigma_5(d)u(n/d)\\ &= [(N^5 * u) * u](n)\\ &= [(u * u) * N^5](n)\\ &= \sum_{d|n}\sigma_0(n/d)^5\\ &= n^5\sum_{d|n}\sigma_0/d^5\end{aligned}$$

Prove that

$$\sum_{d|n}\sigma_1(d)\sigma_1(n/d) = \sum_{d|n} d\sigma_0(d)\sigma_0(n/d)$$

$$\begin{aligned}\sum_{d|n}\sigma_1(d)\sigma_1(n/d) &= [(N * u) * (N * u)](n)\\ &= [(N * N) * (u * u)](n)\end{aligned}$$

With

$$\begin{aligned}[N * N](n) &= \sum_{d|n} d\cdot(n/d) = n\sum_{d|n} 1 = n\sigma_0\\ &= [(n\sigma_0) * (u * u)](n)\\ &= \sum_{d|n} n\cdot(d/n)\sigma_0(n/d)\\ &= \sum_{d|n} d\sigma_0(n/d)\end{aligned}$$

Does

$$4|\sigma_1(4k+3)$$

With $n = 4k+3$ it will have a prime factor of $p = 4t+3$. Recall that $n = p_1^a p_2^b..p_s^t$ we can say that $n = p^r m$ where r is odd and $p \not| m$ Thus we have:

$$\begin{aligned}4|\sigma_1(p^r m) &= 4|sigma_1(m)\sigma_1(p^r)\\ &= 4|\sigma_1(m)(1+p+p^2+...+p^r)\\ &= 4|\sigma_1(m)(1+p)(1+p^2+...+p^{r-1})\\ &= 4|(1+p)(...)\\ &= 4|(1+4t+3)(...)\\ &= 4|4(t+1)(...)\end{aligned}$$

Therefore it is true for all values k

Mersenne prime If $2^n - 1$ is prime then n is prime:
proof
If n is not prime then $n = km$. Using the fact that:

$$a^n - b^n = (a-b)(a^{n-1}b^0 + a^{n-2}b^1 + ... + a^1b^{n-2}a^0b^{n-1})$$

For $a^n - b^n$ to be prime and with $b = 1$, $(a-b) = (a-1) = 1$ therefore $a = 2$
With $n = km$ where $1 < k < n$, $1 < m < n$

$$2^{km} - 1^{km} = (2^k - 1^k)(2^{k(m-1)}1^{0k} + 2^{k(n-2)}1^{1k} + ... + 2^{1k}1^{k(n-2)}2^{0k}1^{k(n-1)})$$

which is a composite number. Therefore if n is not prime $2^n - 1$ is not prime, By Proof by contraposition, if $2^n - 1$ is prime, n must also be prime

Chapter 3

Big-O

$$f(x) = O(g(x))$$

means that there exists a such that:
$g(x) > 0$ for all $x \geq a$
there exists a constant M such that $|f(x)| \leq Mg(x)$ for all $x \geq a$

A common usage is with $f(x) = g(x) + O(h(x))$ that is, we know $f(x)$ is approximately $g(x)$ with a remainder not larger than $h(x)$.
i.e.
$5x^3 - 7x^2 + x = O(x^3)$
$x = O(x^4)$
$sin(x) = O(1)$
$\log(\sqrt{x}) = O(\log(x))$
$\frac{x-\sqrt{x}}{2} \neq O(\sqrt{x})$

Euler Summation

$$\sum_{1 \leq n \leq x} f(n) = \int_1^x f(t)dt + \int_1^x (t - [t])f'(t)dt + f(1) - (x - [x])f(x)$$

where $[x]$ means floor x which is the greatest integer $< x$
With $N = [x]$

$$\begin{aligned}\int_1^x [t]f'(t) &= \int_1^2 f'(t) + 2\int_2^3 f'(t) + ... + (N-1)\int_{N-1}^N f'(t) + N\int_N^x f'(t) \\ &= (f(2) - f(1)) + 2(f(3) - f(2)) + ... + (N-1)(f(N) - f(N-1)) + N(f(x) - f(N)) \\ &= -f(1) - f(2) - ... - f(N-1) + Nf(x) \\ &= -\sum_{1 \leq n \leq x} f(n) + [x]f(x)\end{aligned}$$

when $f(x) = 1$:
$f(t) = 1, \quad f'(t) = 0$

$$\sum_{1 \leq n \leq x} f(n) = 1 + 1 + 1 + ... = [x]$$

$$\int_1^x 1dt + \int_1^x (t - [t])0)dt + 1 - (x - [x])1$$

$$\begin{aligned}&= [t]_1^x + 0 + 1 - x + [x] \\ &= x - 1 + 1 - x + [x] \\ &= [x]\end{aligned}$$

when $f(x) = x$:
$f(t) = t, f'(t) = 1$

$$\sum_{1 \le n \le x} f(n) = 1 + 2 + 3 + ... + x = \frac{[x](x+1)}{2}$$

$$\begin{aligned}
&\int_1^x t dt + \int_1^x (t - [t]) 1 dt + 1 - (x - [x])x \\
=&\int_1^x t dt + \int_1^x t dt - \int_1^x [t] dt + 1 - (x - [x])x \\
=&2[\frac{t^2}{2}]_1^x + 1 - x^2 + [x]x - \int_1^x [t] dt \\
=&[t^2]_1^x + 1 - x^2 + [x]x - \int_1^x [t] dt \\
=&x^2 - 1 + 1 - x^2 + [x]x - \int_1^x [t] dt \\
=&[x]x - \int_1^x [t] dt \\
=&[x]x + \sum_{1 \le n \le x} f(n) - [x]f(x) \\
=&[x]x + \frac{[x](x+1)}{2} - [x]x \\
=&\frac{[x](x+1)}{2}
\end{aligned}$$

Euler Summation with big O

$$\sum_{2 \le n \le x} \frac{1}{n \log n}$$

With

$$\sum_{y \le n \le x} f(n) = \int_y^x f(t) dt + \int_y^x (t - [t]) f'(t) dt + [y - [y]] f(y) - (x - [x]) f(x)$$

Therefore

$$\sum_{2 \le n \le x} \frac{1}{n \log n} = \int_2^x \frac{1}{t \log t} dt + \int_2^x (t - [t]) \left(\frac{1}{t \log t} \right)' dt + [y - [y]] \frac{1}{2 \log 2} - (x - [x]) \frac{1}{x \log x}$$

Using the fact that $[x - [x]] < 1$, $(x - [x]) \frac{1}{x \log x} = O\left(\frac{1}{x \log x} \right)$
and $[y - [y]] \frac{1}{2 \log 2} = \frac{1}{2 \log 2}$

we can now look at the first integral. Using integration by substitution: Setting $u = \log t$, $du/dt = 1/t$ giving:

$$\int_2^x \frac{1}{t \log t} dt = \int_{\int 2du}^{\int xdu} \frac{1}{u} \frac{du}{dx} dx = \int_{\log 2}^{\log x} \frac{1}{u} du$$

Giving

$$\log \log x - \log \log 2$$

Now for the second integral. Note that $\frac{1}{x \log x}$ is positive decreasing $\to 0$ as $x \to \infty$ so its derivative is negative decreasing towards 0.
Separating the integral into parts:

$$\int_2^x (t - [t]) \left(\frac{1}{t \log t} \right)' dt = \int_2^\infty (t - [t]) \left(\frac{1}{t \log t} \right)' dt - \int_x^\infty (t - [t]) \left(\frac{1}{t \log t} \right)' dt$$

For the 1st part we can see that the value will be negative and decreasing, giving $| - f(\infty)' + f(2)'| \leq f(2)'$ thus is some constant K

The second part is:

$$\left| \int_x^\infty (t - [t]) \left(\frac{1}{t \log t} \right)' dt \right| \leq \int_x^\infty \left| \left(\frac{1}{t \log t} \right)' \right| dt = O\left(\frac{1}{x \log x} \right)$$

as $\frac{1}{x \log x} \to 0$ as $x \to \infty$ Putting it all together we have:

$$\log \log x - \log \log 2 + K + \frac{1}{2 \log 2} + O\left(\frac{1}{x \log x} \right)$$

Show that

$$\phi(n) = \frac{3}{\pi^2} x^2 + O\left(x \log x \right)$$

With

$$\phi(n) = \sum_{n \leq x} \sum_{d | n} \mu(d) \frac{n}{d}$$

we can show this in the form of a table. Suppose $x = 10$

		n(=qd)									
		1	2	3	4	5	6	7	8	9	10
	1	1, 1	2, 1	3, 1	4, 1	5, 1	6, 1	7, 1	8, 1	9, 1	10, 1
	2		1, 2		2, 2		3, 2		4, 2		5, 2
	3			1, 3			2, 3			3, 3	
	4				1, 4				2, 4		
d	5					1, 5					2, 5
	6						1, 6				
	7							1, 7			
	8								1, 8		
	9									1, 9	
	10										1, 10

Each cell within the table contains the numbers (q, d) where $qd \leq x$

We can see that the first sum $\sum_{d|n} \mu(d)\frac{n}{d}$ for each n can be attained by the totalling the n column. e.g $\sum_{d|6} \mu(d)\frac{6}{d} = 1 \cdot 6 + 2 \cdot 3 + 3 \cdot 2 + 6 \cdot 1$
The 2nd part of the sum $\sum_{n \leq x} ...$ is the total of all the columns.

Another way of writing this is that it is the sum of each cell within the table, that is:

$$\phi(n) = \sum_{n \leq x} \sum_{d|n} \mu(d)\frac{n}{d} = \sum_{\substack{q,d \\ qd \leq x}} \mu(d)q$$

This shows that instead of having to take the sums of the columns, we can take the sums of the rows.
The sum of a row is shown as $\sum_{q \leq \frac{x}{d}} \mu(d)q$ and the sum of all rows is $\sum_{d \leq x} ...$ giving:

$$\sum_{d \leq x} \sum_{q \leq \frac{x}{d}} \mu(d)q$$

As $\mu(d)$ is independent of the 1st summation (it is fixed for q) we can rewrite it as

$$\sum_{d \leq x} \mu(d) \sum_{q \leq \frac{x}{d}} q$$

Using theorem 3.2(d) where $\sum_{n \leq x} n = \frac{1}{2}x^2 + O(x)$ Replacing n with q and x with $\frac{x}{d}$

$$\sum_{q \leq \frac{x}{d}} q = \frac{1}{2}\left(\frac{x}{d}\right)^2 + O\left(\frac{x}{d}\right)$$

Thus

$$\sum_{d \leq x} \mu(d) \left(\frac{1}{2}\left(\frac{x}{d}\right)^2 + O\left(\frac{x}{d}\right)\right)$$

With $\mu(d) = O(1)$ and x being independent of the summation we get

$$\frac{1}{2}x^2 \sum_{d \leq x} \frac{\mu(d)}{d^2} + O\left(x \sum_{d \leq x} \frac{1}{d}\right)$$

Using the formula in chapter 3.7, where

$$\sum_{n \leq x} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2} + O\left(\frac{1}{x}\right)$$

substituting n to d we therefore get

$$\frac{1}{2}x^2\left(\frac{6}{\pi^2} + O\left(\frac{1}{x}\right)\right) + O\left(x \sum_{d \leq x} \frac{1}{d}\right) = \frac{3}{\pi^2}x^2 + O(x) + O\left(x \sum_{d \leq x} \frac{1}{d}\right)$$

then using theorem 3.2(a)

$$\sum_{n\leq x}\frac{1}{n}=\log x+C+O\left(\frac{1}{x}\right)$$

Again substituting n to d we therefore get

$$\frac{3}{\pi^2}x^2+O\left(x\right)+O\left(x\left(\log x+C+O\left(\frac{1}{x}\right)\right)\right)$$

$$=\frac{3}{\pi^2}x^2+O\left(x\right)+O\left(x\log x+xC+O\left(x\right)\right)$$

$$=\frac{3}{\pi^2}x^2+O(x\log x)$$

$$\sum_{n\leq x}d(n)=2\sum_{d\leq\sqrt{x}}\left\{\left[\frac{x}{d}\right]-d\right\}+[\sqrt{x}]$$

Legrendre's Identity Theorem 3.14 shows that:

$$[x]!=\prod_{p\leq x}p^{\alpha(p)}$$

where

$$\alpha(p)=\sum_{m=1}^{\infty}\left[\frac{x}{p^{\alpha}}\right]$$

Example:
Find the highest power of 3 dividing 823! We have $p=3^{\alpha}$ giving

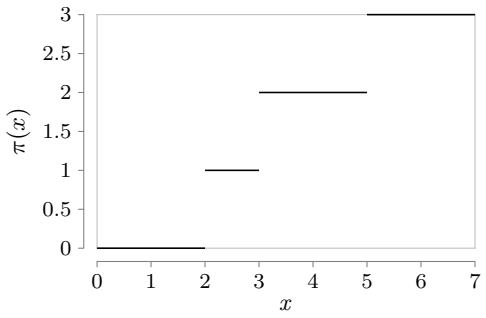
$$\alpha(p)=\left[\frac{823}{3}\right]+\left[\frac{823}{9}\right]+\left[\frac{823}{27}\right]+\left[\frac{823}{81}\right]+\left[\frac{823}{243}\right]+\left[\frac{823}{729}\right]=274+91+30+10+3+1=409$$

This the highest power is $\alpha=409$

1 Chapter 4

Number of primes satisfying $p \leq x$

$$\pi(x) = \sum_{p \leq x} 1$$



Chebyshev's Functions

$$\vartheta(x) = \sum_{p \leq x} \log p$$

For $x \geq 2$ we have

$$\vartheta(x) = \pi(x)\log(x) - \int_2^x \frac{\pi(x)}{t} dt$$

that is ϑ add $\log p$ for every prime p For $x = 6.5$ we have

$$\begin{aligned}
&\pi(6)\log(6.5) - \int_2^6 \frac{\pi(x)}{t} dt \\
=&3\log(6.5) - \int_2^3 \frac{1}{t} - \int_3^5 \frac{2}{t} - \int_5^{6.5} \frac{3}{t} dt \quad \text{(as per graph above)} \\
=&3\log(6.5) - (\log(3) - \log(2)) - 2(\log(5) - \log(3)) - 3(\log(5) - \log(6.5)) \\
=&\log(2) + log(3) + log(5) \\
=&\vartheta(6.5)
\end{aligned}$$

$$\psi = \sum_{n \leq x} \Lambda(n)$$

that is ψ adds $\log p$ for every power of p.

Th 15

$$0 \leq \frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \leq \frac{(\log x)^2}{2\sqrt{x}\log 2}$$

th=ells us that asymptotically (approaching a given value as an expression containing a variable tends to infinity) that ϑ and ψ behave similarly, also RHS tends to zero as $x \to \infty$ Aim of Chapter 4 is to relate $\pi(x)$ and $\vartheta(x)$, bringing about the Prime Number Theorem (PMT).

theorem 4.4

$$\lim_{x\to\infty} \frac{\pi(x)\log(x)}{x} = 1$$

$$\lim_{x\to\infty} \frac{vartheta(x)}{x} = 1$$

$$\lim_{x\to\infty} \frac{psi(x)}{x} = 1$$

This comes about from

$$\vartheta(x) = \pi(x)\log x - \int_2^x \frac{\pi(t)}{t}dt$$

$$\pi(x) = \int_2^x \frac{\vartheta(t)}{t\log^2 t}dt$$

which uses Abel's Identity

2 Abel's Identity

For any arithmetical function $a(n)$ we have:

$$\sum_{y<n\leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt$$

where

$$A(x) = \sum_{n\leq x} a(n)$$

and f has a continuous derivative on $[y, x]$.

Example
Prove that

$$\sum_{n\leq x} a(n) = \frac{B(x)}{\log x} + \int_2^x \frac{B(t)}{t\log^2 t}dt$$

and deduce that if $B(t) = O(t)$ then

$$\sum_{n \leq x} = O\left(\frac{x}{\log x}\right)$$

Knowing that $f(x) = \frac{1}{\log x}$ we deduce that $b(n) = a(n) \log n$ to give

$$\sum_{n \leq x} a(n) = \frac{B(x)}{\log x} + \int_2^x \frac{B(t)}{t \log^2 t} dt$$

With $B(t) = O(t)$

$$\int_2^x \frac{B(t)}{t \log^2 t} dt = O\left(\int_2^x \frac{1}{\log^2 t} dt\right)$$

Splitting this up into

$$O\left(\int_2^x \frac{1}{\log^2 t} dt\right) = O\left(\int_2^{\sqrt{x}} \frac{1}{\log^2 t} dt\right) + O\left(\int_{\sqrt{x}}^x \frac{1}{\log^2 t} dt\right)$$

With

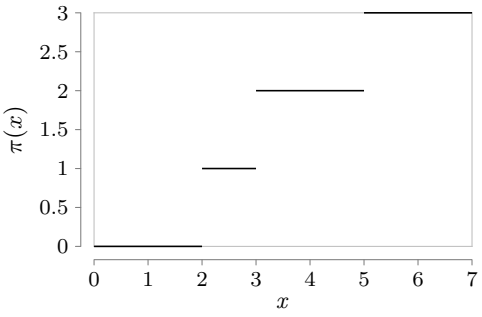
$$\int_2^{\sqrt{x}} \frac{1}{\log t} dt \leq \int_2^{\sqrt{x}} \frac{1}{\log 2} dt = \frac{1}{\log 2}(\sqrt{x} - 2) \leq \frac{\sqrt{x}}{\log 2}$$

we have

$$O\left(\frac{\sqrt{x}}{\log^2 2}\right) + O\left(\frac{x}{\log^2 \sqrt{x}}\right) = O(\sqrt{x}) + O\left(\frac{x}{\log^2 x}\right) = O\left(\frac{x}{\log^2 x}\right)$$

3 examples

Let $\vartheta_1(x) = \int_1^x \vartheta(t) dt$ Calculate $\vartheta_1(6.5)$ Drawing the graph for $\vartheta(x) = \sum_{p \leq x} \log p$



and breaking integral up accordingly we get

$$\begin{aligned}
\vartheta_1(x) &= \int_1^x \vartheta(t)dt \\
&= \int_1^2 \vartheta(t)dt + \int_2^3 \vartheta(t)dt + \int_3^5 \vartheta(t)dt + \int_5^{6.5} \vartheta(t)dt \\
&= 0 + \log 2 + 2 \cdot (\log 2 + \log 3) + \frac{3}{2}(\log 2 + \log 3 + \log 5) \\
&= \frac{9}{2}\log 2 + \frac{7}{2}\log 3 + \frac{3}{2}\log 5
\end{aligned}$$

The multiplier comes from the size of the x-axis, the logs are the sums of the $\log p$ from 1 to x

Let $\Lambda_1(n) = \log n$ if n is prime, 0 otherwise. Prove that
$\vartheta_1(x) = \sum_{n \leq x}(x-n)\Lambda_1(n)$

We have a summation with $f(n)a(n)$ so we can use Abel's identity.
page 78 shows that $\vartheta(x) = \sum_{p \leq x} \log p$ thus $a(n) = \log n = \Lambda_1(n)$ and $A(n) = \vartheta(n)$. Setting $f'(x) = 1$ gives $f(x) = x$

$$\begin{aligned}
\sum_{n \leq x} a(n)f(n) &= f(x)A(x) - \int_1^x A(t)f'(t)dt \\
\sum_{n \leq x} \Lambda_1(n)n &= x\vartheta(x) - \int_1^x \vartheta(t)dt \\
\sum_{n \leq x} \Lambda_1(n)n &= x\vartheta(x) - \vartheta_1(x) \\
\sum_{n \leq x} n\Lambda_1(n) &= x\sum_{n \leq x} \Lambda_1(n) - \vartheta_1(x) \\
\vartheta_1(x) &= x\sum_{n \leq x} \Lambda_1(n) - \sum_{n \leq x} n\Lambda_1(n) \\
\vartheta_1(x) &= \sum_{n \leq x}(x-n)\Lambda_1(n)
\end{aligned}$$

With $x = 6.5$ we have

$$\begin{aligned}\vartheta_1(x) &= \sum_{n \leq x} (x-n)\Lambda_1(n) \\ &= (6.5-1)\Lambda(1) + (6.5-2)\Lambda(2) + (6.5-3)\Lambda(3) \\ &+ (6.5-4)\Lambda(4) + (6.5-5)\Lambda(5) + (6.5-6)\Lambda(6) \\ \\ &= (5.5)\cdot 0 + (4.5)\log(2) + (3.5)\log(3) + (2.5-4)\cdot 0 \\ &+ (1.5)\Lambda(5) + (0.5-6)\cdot 0 \\ \\ &= \frac{9}{2}\log(2) + \frac{7}{2}\log(3) + \frac{3}{2}\Lambda(5)\end{aligned}$$

showing that it matches with the answer to part 1 of the question

4 Equivalence

$$f(x) \sim g(x) \Rightarrow \lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$$

That is, f and g grow at the same rate, whereas $f(x) = O(g(x))$ says that f grows *no faster* than g. $f(x) \sim g(x)$ means that $f(x) = O(g(x))$ but not the other way around

5 Little o

$$f(x) = o(g(x)) \Rightarrow \lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$$

That is, $g(x)$ grows much faster than $f(x)$.

$$|f(x)| \leq \varepsilon g(x)$$

The difference between little-o and big-O is that whilst the latter has to be true for at least one constant M the former has to hold for every positive constant ε.
e.g. $2x = o(x^2)$ and $1/x = o(1)$

6 Order of Common Functions

$O(1) \to O(\log\log n) \to O(n^c)_{c<1} \to O(n) \to O(n\log n) \to O(n^c)_{c>1} \to O(c^n) \to O(n!)$

Linear Congruence

To find if there is a solution to a linear congruence in the form $ax \equiv b \pmod{c}$ we need to find the highest common factor (HCF) of (a, c) and see if this is a divisor of b. For instance:

$14x \equiv 7 \pmod{8}$
$\text{HCF}(14, 8) = 2$, 2 is not a divisor of 7, therefore there are no solutions.

$21x \equiv 3 \pmod{5}$
$\text{HCF}(21, 5) = 1$, 1 is a divisor of 3, therefore there are solutions

Complete Residue Function

A complete residue function is one where you have every remainder within the set. For instance:

$$\{0, 1, 2, 3, 4\} \pmod{5}$$
$$\{11, 12, 13, 14, 15, 21, 25, 2878\} \pmod{5}$$

Reduced Residue Function

A reduced residue function will be a set with $\phi(p)$ values which are all relatively prime to p. For instance, with $\pmod{6}$, $\phi(6) = 2$ so the set is $\{1, 5\}$ or $\{5, 7\}$ $\pmod{6}$

Finding x

To find x you can either:

- multiply by a number relatively prime to m
- replace a or b by a congruent number
- cancel any common divisor of a and b

For example, $4x \equiv 5 \pmod{7}$:
Multiply by 2 to give

$$8x \equiv 10 \pmod{7}$$
$$x \equiv 3 \pmod{7}$$

or add 7 to 5

$$4x \equiv 12 \pmod 7$$

then divide by 4 to give

$$x \equiv 3 \pmod 7$$

or to get $-x$ we note that $21 \equiv 0 \pmod 7$ so multiplying by 5 gives

$$20x \equiv 25 \pmod 7$$

$$-x \equiv 4 \pmod 7$$

$$x \equiv -4 \equiv 3 \pmod 7$$

If we have something like $18x \equiv 39 \pmod{69}$ in which we can divide everything by 3 to give

$$6x \equiv 13 \pmod{23}$$

multiply a and b by 4 to give

$$24x \equiv 52 \pmod{23}$$

$$x \equiv 6 \pmod{23}$$

But as this is the solution for $\pmod{23}$ and we started with $\pmod{69}$, due to dividing by 3, this means there are in fact 3 answers.
These are

$$6,\ 6+23,\ 6+2\cdot 23 = 6,\ 29,\ 52$$

unique mod m

If $(a, m) = 1$ the solution to $ax \equiv b \pmod m$ is

$$x \equiv ba^{\varphi(m)-1} \pmod m$$

with φ being the Euler totient.

For instance, solve the congruence $5x \equiv 3 \pmod{24}$
Since $(5, 24) = 1$ there is a unique solution. Therefore

$$x \equiv 3 \cdot 5^{\varphi(24)-1}$$

$$\varphi(24) = \varphi(3)\varphi(8) = 2 \cdot 4 = 8$$

giving

$$x \equiv 3 \cdot 5^7 \pmod{24}$$

With

$$5^2 \equiv 1 \text{ meaning that } 5^6 = 5^2 \cdot 5^2 \cdot 5^2 \equiv 1 \cdot 1 \cdot 1 \equiv 1$$

This gives

$$5^7 = 5 \cdot 5^6 \equiv 5 \cdot 1 \equiv 5 \pmod{24}$$

Thus

$$x \equiv 3 \cdot 5^7 \equiv 3 \cdot 5 \equiv 15 \pmod{24}$$

So

$$x \equiv 15 \pmod{24}$$

Chinese Remainder Theorem

The chinese remainder theorem works on multiple linear congruences that are relatively prime to each other.
The quickest way is to leave the easiest multiple moduli to last i.e. $\pmod 5$ or $\pmod 2$. otherwise start with the two largest, find a solution by adding the modulus to the value, multiply the modulus and find a solution. e.g.

$$\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 6 \pmod 7 \\ x &\equiv 5 \pmod{11} \end{aligned}$$

All moduli are relatively prime, so we start with the two highest.

$$\begin{aligned} x &\equiv 6 \pmod 7 = 6, 13, 20, 27, ... \\ x &\equiv 5 \pmod{11} = 5, 16, 27, ... \end{aligned}$$

so $27 \equiv \pmod 7$ and $\pmod{11}$, therefore $x \equiv 27 \pmod{7 \cdot 11} = \pmod{77}$.
Checking the last congruence with the new congruence.

$$\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 27 \pmod{77} = 27, 104, ... \end{aligned}$$

knowing that $4 \equiv 104 \pmod 5$ we have the answer

$$x = 104$$

CRT for non-coprime moduli

With

$$\begin{aligned} x &\equiv b_1 \pmod{m_1}, \\ x &\equiv b_2 \pmod{m_2}, \\ &..., \\ x &\equiv b_r \pmod{m_r} \end{aligned}$$

has a simultaneous solution iif $gcd(m_i, m_j)$ divides $b_i - b_j$ for every pair $i \neq j$.

Examples With

$$\begin{aligned} x &\equiv 7 \pmod{12}, \\ x &\equiv 11 \pmod{18}, \\ x &\equiv 1 \pmod{23} \end{aligned}$$

$gcd(12, 18) = 6$ but $7-11 = -4$ which is not divisible by 6, so it has no solutions.
With

$$\begin{aligned} x &\equiv 3 \pmod 7, \\ x &\equiv 4 \pmod{12}, \\ x &\equiv 10 \pmod{18} \end{aligned}$$

$gcd(12, 18) = 6$ and $4 - 10 = -6$ which divides 6, and 7 is coprime to 12 and 18 so there is a solution.

$$\begin{aligned} x &\equiv 4 \pmod{12} = 4, 16, 28, ... \\ x &\equiv 10 \pmod{18} = 10, 28, ... \end{aligned}$$

so $x \equiv 28 \pmod{12}$ and $\pmod{18}$.
Find $lcm(12, 18) = 36$ we have $x \equiv 28 \pmod{36}$

$x \equiv 3 \pmod 7 = 3, 10, 17, 24, 31, 38, 45, 52, 59, ..., 136 x \equiv 28 \pmod{36} = 28, 64, 100, 136$

thus we have

$$x \equiv 136 \pmod{7 \cdot 36 = 252}$$

Polynomial congruences with composite moduli For $f(x) = x^2 + 5x + 24 \equiv 0 \pmod{75}$
75 is a composite of $3 \cdot 25 = 3 \cdot 5^2$, therefore we find $f(x) \equiv 0 \pmod 3$ and $f(x) \equiv \pmod 5$

$$\begin{aligned} x^2 + 5x + 24 &\equiv 0 \pmod 3 \\ x^2 + 2x &\equiv 0 \pmod 3 \\ x^2 - x &\equiv 0 \pmod 3 \\ x &= 0 \text{ or } 1 \end{aligned}$$

$$\begin{aligned} x^2 + 5x + 24 &\equiv 0 \pmod 5 \\ x^2 - 1 &\equiv 0 \pmod 5 \\ x &= 1 \text{ or } 4 \end{aligned}$$

For $p = 5,\ \alpha = 2$ assume that $f'(r) \not\equiv 0 \pmod 5$, then r can be lifted from 5 to 25.

$$\begin{aligned} f'(r) &= 2x + 5 \not\equiv 0 \pmod 5 \\ f'(1) &= 2 + 5 = 2 \not\equiv 0 \pmod 5 \\ f'(4) &= 8 + 5 = 3 \not\equiv 0 \pmod 5 \end{aligned}$$

Lifting r to $a = r + qp^{\alpha-1}$
obtain k from $f(r) = kp^{\alpha-1}$

obtain q from $qf'(r) + k \equiv 0 \pmod{p}$
obtain a from $a = r + qp^{\alpha-1}$

For $r = 1$

$$\begin{aligned} f(1) = 30 &= k5 \\ \therefore k &= 6 \\ qf'(1) + 6 = q(2+5) + 6 &= 2q + 1 \equiv 0 \pmod{5} \\ = 2q - 4 &\equiv \pmod{5} \\ \therefore q &\equiv 2 \pmod{5} \\ a &= 1 + 2 \cdot 5 = 11 \end{aligned}$$

Thus the solution is $11 \pmod{25}$

For $r = 4$

$$\begin{aligned} f(4) = 60 &= k5 \\ \therefore k &= 12 \\ qf'(4) + 12 = q(8+5) + 12 &= 3q + 2 \equiv 0 \pmod{5} \\ \therefore q &\equiv 1 \pmod{5} \\ a &= 4 + 1 \cdot 5 = 9 \end{aligned}$$

Thus the solution is $9 \pmod{25}$

So far we have the solutions 0 and 1 (mod 3), and 9 and 11 (mod 25). We now need to solve these in pairs as simultaneous equations.

$$\begin{aligned} x &\equiv 9 \pmod{25} \\ x &\equiv 0 \pmod{3} \\ 9 &\equiv 0 \pmod{3} \end{aligned}$$

so $x = 9$

$$\begin{aligned} x &\equiv 9 \pmod{25} \\ x &\equiv 1 \pmod{3} \\ 9 + 25 \equiv 34 &\equiv 1 \pmod{3} \end{aligned}$$

so $x = 34$

$$\begin{aligned} x &\equiv 11 \pmod{25} \\ x &\equiv 0 \pmod{3} \\ 11 + 25 \equiv 36 &\equiv 0 \pmod{3} \end{aligned}$$

so $x = 36$

$$\begin{aligned} x &\equiv 11 \pmod{25} \\ x &\equiv 1 \pmod{3} \\ 11 + 25 \equiv 36 + 25 \equiv 61 &\equiv 1 \pmod{3} \end{aligned}$$

so $x = 61$
So for $f(x) = x^2 + 5x + 24 \equiv 0 \pmod{75}$ the solutions are:

$$x = 9,\ x = 34,\ x = 36,\ x = 61$$

Hansel's Lemma

Find a root a_0 of f modulo p i.e. $f(a_0) \equiv 0 \pmod{p}$
Calculate $f'(a_0)$ and $g = f'(a_0)^{-1} \pmod{p}$
For $r = 0, 1, ...$ compute $a_r - f(a_r)g \pmod{p^{r+1}}$

Find all the roots of $5x^3 + x^2 - 1 \equiv 0 \pmod{125}$

we have $125 = 5^3$ so we need to work in $\pmod 5$ and lift twice.

$$5x^3 + x^2 - 1 \equiv x^2 - 1 \equiv 0 \pmod{5}$$

giving $x = 1$ and $x = 4$
Next we check $f'(x)$ to see if it can be lifted

$$\begin{aligned} f'(x) &= 2x \pmod{5} \\ f'(1) &= 2 \not\equiv 0 \pmod{5} \\ f'(4) &= 8 \equiv 3 \not\equiv 0 \pmod{5} \end{aligned}$$

telling us that both solutions are non-singular and thus can be lifted uniquely.

Next we need to calculate $f'(a_r)$ and $q = f'(a_r)^{-1} \pmod{p}$ (only needed to be done once for repeated lifts). Then compute

$$a_r - f(a_r)q \pmod{p^{r+1}}$$

For $x = 1$ $f'(1) = 2$ so $f'(1)^{-1} = 3$ giving

$$1 - (5 \cdot 1^3 + 1^2 - 1) \cdot 3 = -14 \equiv 11 \pmod{25}$$

Lifting again:

$$11 - (5 \cdot 11^3 + 11^2 - 1) \cdot 3 = -20314 \equiv 61 \pmod{125}$$

For $x = 4$ $f'(4) = 3$ so $f'(4)^{-1} = 2$ giving

$$4 - (5 \cdot 4^3 + 4^2 - 1) \cdot 2 = -666 \equiv 9 \pmod{25}$$

Lifting again:

$$9 - (5 \cdot 9^3 + 9^2 - 1) \cdot 2 = -7441 \equiv 59 \pmod{125}$$

Thus $x = 59, 61 \pmod{125}$

If we have $\pmod{50}$ where $50 = 2 \cdot 5^2$ we will work out $\pmod 2$ and $\pmod 5$, lift 5 to $\pmod{25}$, then say if we have two answers for $\pmod 2$, say a and b and two for $\pmod{25}$, say c and d then we will get 4 answers,

$$\begin{aligned} x &\equiv a \pmod 2 \\ x &\equiv c \pmod{25} \end{aligned}$$

$$\begin{aligned} x &\equiv a \pmod 2 \\ x &\equiv d \pmod{25} \end{aligned}$$

$$\begin{aligned} x &\equiv b \pmod 2 \\ x &\equiv c \pmod{25} \end{aligned}$$

$$\begin{aligned} x &\equiv b \pmod 2 \\ x &\equiv d \pmod{25} \end{aligned}$$

Euler-Fermat Theorem Th5.17

$$a^{\phi(m)} \equiv 1 \pmod m$$

Th5.18 - If a prime does not divide a then

$$a^{p-1} \equiv 1 \pmod p$$

Little Fermat Theorme For any integer a and any prime p we have

$$a^P \equiv a \pmod p$$

Th5.20 - If $(a, m) = 1$ the solution of the linear congruence

$$ax \equiv b \pmod m$$

is given by

$$x \equiv ba^{\phi(m)-1} \pmod m$$

Wilson's Theorem For any prime p we have

$$(p-1)! \equiv -1 \pmod{p}$$

conversely if $(n-1)! \equiv -1 \pmod{n}$ then n is prime.

Chapter 6

Finite Abelian and their characters - The 4 group postulates

A group G is a nonempty set of elements with a binary operation

(a) Closure - For every a in G, $a \cdot b$ is also in G

(b) Associativity - For every a,b,c in G $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(c) Existence of identity there is a unique element e in G called the identity such that $a \cdot e = e \cdot a = a$ for every a in G

(d) Existance of inverses - $a \cdot b = b \cdot a = e$ where $b = a^{-1}$

A group is called Abelian if $ab = ba$
A group G is finite if G is a finite set. In this case the number of elements in G is called the order of G, denoted by $|G|$
A subgroup of G is a non empty subset G' which itself is a group under the same operation. Every group has 2 subgroups, G itself and the set e consisting of the identity element alone.
G' is a subgroup only if

(a) Closure- if $a, b \in G'$ then $ab \in G'$

(b) Existence of inverse - If $a \in G'$, then $a^{-1} \in G'$

Note that if the binary operation on G is addition (+), we usually write 0 instead of e, $a + b$ instead of ab, and $-a$ instead of a^{-1}
Also if G is a group under the operation of addition, then Theorem 6.1 states that: if $a + c = b + c$ or $c + a = c + b$, then $a = b$

Characters of finite abelian group

A complex valued function f defined on G is called a character of G if f has the multiplicative property

$$f(ab) = f(a)f(b)$$

for all $a, b \in G$ and if $f(c) \neq 0$ for some c in G

If f is a character of a finite group G with identity element e then $f(e) = 1$. If $a^n = e$ then $f(a)^n = 1$

eg Let G be the group $\pmod 7$ then

$$f(1) = f(2) = f(4) = 1$$

as $e = 1$, $2^3 \equiv 1$ and $4^3 \equiv 1$ likewise

$$f(3) = f(5) = f(6) = -1$$

A finite Abelian group of order n has exactly n characters.
A subgroup of G is G'. A new subgroup containing G' and at least one more element not in G' is denoted as $< G'; a >= \{xa^k : x \in G' \text{and} 0 \leq k \leq h\}$ where h is the indicator of a in G'
Applying this theory starting with the subgroup $\{e\}$ denoted as $G_1 \neq G$ and adding another element a_1 in G but not in G_1, and defining this as G_2 we get $G_2 =< G_1; a_1 >$
Continuing this until we have have all the element in G we get $G_{r+1} =< G_r; a_r >$
With $G_1 \subset G_2 \subset ... \subset G_{t+1} = G$

the character group

If $f_i f_j)(a) = f_i(a) f_j(a)$
for each a in G then the set of characters of G forms an Abelian group of order n. We denote this group as $\hat{G}$. The identity element of $\hat{G}$ is denoted by f_1, with the others denoted by $f_2, f_3..., f_n$ known as non principal characters. They have the property that $f(a) \neq 1$ for some a in G. The inverse of f_i is the reciprocal $1/f_i$.
Note for each character f we have $|f(a)| = 1$ Hence the reciprocal $1/f(a)$ is equal to the complex conjugate $\overline{f(a)}$

$$\overline{f(a)} = \overline{f}(a) = \frac{1}{f(a)} = f(a^{-1}$$

Defining A =A(G) as a $n \times n$ matrix whose element $a_{ij} = f_i(a_j)$

Dirichlet characters

Let G be the group of reduced residue classes modulo k. With $\phi(k) = f$ we have χ_1 to χ_f
If $(n, k) = 1$ then $\chi(n)$ is a character f within the residue class of G, that is $\chi(n) = f(\hat{n})$ and 0 otherwise.

If G is cyclic then each character f can be expressed as a power of a generator character.
For instance the group G_{10} the order $n = \phi(10) = \phi(2)\phi(5) = 1 \cdot 4 = 4$ where the relatively prime numbers are $\{1, 3, 7, 9\}$
Now 1 can not be the generator as $1^k = 1$ but $3^1 = 3$, $3^2 = 9$, $3^3 \equiv 7$ and $3^4 \equiv 1$ thus each element can be produce by 3^k, giving the set $\{1, 3, 7, 9\} = \{3^4, 3, 3^3, 3^2\} = \{3, 3^2, 3^3, 3^4\}$

So to create a Cayley table once we have worked out the values for $\chi(3)$ we can get any value $\chi(g)$.
Now we know that the identity character $f(e) = 1$, where $e = 1$ so $\chi(1) = 1$, but we also know that $3^4 = 1$, so $\chi(3)^4 = \chi(3^4) = 1$. This means that there are 4 solutions in the complex plane, namely $\{1, -1, i, -i\}$

Next fill out the Cayley table where any element which is not a prime = 0, $\chi_1(n) = 1$ otherwise, and add the values for the column $n = 1$ to be 1 and $n = 3$ to be the 4 solutions to the complex plane.

n	1	2	3	4	5	6	7	8	9	10
$\chi_1(n)$	1	0	1	0	0	0	1	0	1	0
$\chi_2(n)$	1	0	-1	0	0	0		0		0
$\chi_3(n)$	1	0	i	0	0	0		0		0
$\chi_4(n)$	1	0	$-i$	0	0	0		0		0

With $i^2 = -1$ we can fill in the table for $3^2 = 9$, then for $3^3 = 27 \equiv 7$

n	1	2	3	4	5	6	7	8	9	10
$\chi_1(n)$	1	0	1	0	0	0	1	0	1	0
$\chi_2(n)$	1	0	-1	0	0	0	-1	0	1	0
$\chi_3(n)$	1	0	i	0	0	0	$-i$	0	-1	0
$\chi_4(n)$	1	0	$-i$	0	0	0	i	0	-1	0

Within the Dirichlet character table, each row and each column adds up to 0 individually (not including the e row and column $n = 1$).

For $k = 3$

n	1	2	3
$\chi_1(n)$	1	1	0
$\chi_2(n)$	1	-1	0

For the above $k = 3$, $\phi(3) = 2$ $\{1, 2\}$ so $3 = 0$ within the column. $1 = 1$ within the column. $\chi_1(n) = 1$ within the row. For the value missing in 2, choose a value that makes each row and column = 0 respectively.

$k = 5$ $\phi(5) = 4$, $\{1, 2, 3, 4\}$

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1				0
$\chi_3(n)$	1				0
$\chi_4(n)$	1				0

With $\chi(n)^4 = \chi(n^4) = \chi(1) = 1$ for any value n we know that there must be 4 solutions in the complex plane, namely $\{1, -1, i, -i\}$. With 1 in the 1st row,

we can fill column 2 out with $\{-1, i, -i\}$ in any order.

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1	-1			0
$\chi_3(n)$	1	i			0
$\chi_4(n)$	1	$-i$			0

This is not a cyclic group so we do not have a generating element. So, knowing that $\chi(mn) = \chi(m)\chi(n)$ we have $\chi(1) = 1 = \chi(6) = \chi(3)\chi(2)$ thus 3 is the inverse of 2.

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1	-1	-1		0
$\chi_3(n)$	1	i	$-i$		0
$\chi_4(n)$	1	$-i$	i		0

For 4 we know that $2^2 = 4$ so we can use that to fill in column 4

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1	-1	-1	1	0
$\chi_3(n)$	1	i	$-i$	-1	0
$\chi_4(n)$	1	$-i$	i	-1	0

To ensure that this is correct, check the rows and columns under addition.

7 The non-Vanishing of L

We denote $L(1, \chi)$ by the sum

$$L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}$$

where $L(1, \chi) \neq 0$ when χ is a non-principal character (i.e. $L(1, \chi_1(n)$

For $k = 5$ we have

$$L(1, x_2) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = 1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{4} + \frac{1}{6} - \frac{1}{7} - \frac{1}{8} + \frac{1}{9} + \frac{1}{11} - \frac{1}{12} - \frac{1}{13} + \frac{1}{14} + ...$$

Looking for a sequence for which $L \not\land$ we can show that For $k = 5$ we have

$$L(1, x_2) = 1 - \frac{1}{2} - \frac{1}{3} + \left(\frac{1}{4} + \frac{1}{6} - \frac{1}{7} - \frac{1}{8}\right) + \left(\frac{1}{9} + \frac{1}{11} - \frac{1}{12} - \frac{1}{13}\right) + \frac{1}{14} + ...$$

where the values within the brackets are positive, and $1 - \frac{1}{2} - \frac{1}{3} = \frac{1}{6}$ and therefore positive, showing that indeed $L(1, \chi) \neq 0$

Theorem 6.19

$$A(n) = \sum_{d|n} \chi(d)$$

Then $A(n) \geq 0$ for all n and $A(n) \geq 1$ if n is a square. For $A(225)$ we have the divisors $d = \{1, 3, 5, 9, 15, 25, 45, 75, 225\}$ For $\pmod{16}$ this equates to $d = \{1, 3, 5, 9, 15, 9, 13, 11, 1\}$ Thus

$$A(225) = 2\chi(1) + \chi(3) + \chi(5) + 2\chi(9) + \chi(11) + \chi(13) + \chi(15)$$

An answer is found for all real valued non-principle characters by plugging in the values from the table.
Example:
For each real-valued nonprinciple character χ mod k let

$$A(n) = \sum_{d|n} \chi(d) \qquad F(x) = \sum_{n \leq x} \frac{A(n)}{n}$$

Show that

$$F(x) = L(1, \chi) \log x + O(1)$$

We have

$$A(n) = \sum_{d|n} \chi(d)$$

So the sum of $A(n)$ is

$$\sum_{n \leq x} A(n) = \sum_{n \leq x} \sum_{d|n} \chi(d)$$

Thus we have

$$F(x) = \sum_{n \leq x} \frac{A(n)}{n} = \sum_{n \leq x} \frac{1}{n} \sum_{d|n} \chi(d)$$

With the double summation we can say

$$\sum_{n \leq x} \frac{1}{n} \sum_{d|n} \chi(d) = \sum_{\substack{q,d \\ qd \leq x}} \frac{1}{qd} \chi(d) = \sum_{d \leq x} \frac{\chi(d)}{d} \sum_{q \leq \frac{x}{d}} \frac{1}{q}$$

Theorem 3.2 shows that

$$\sum_{q \leq \frac{x}{d}} \frac{1}{q} = \log \frac{x}{d} + C + O\left(\frac{d}{x}\right)$$

Giving

$$= \sum_{d \leq x} \frac{\chi(d)}{d} \left(\log \frac{x}{d} + C + O\left(\frac{d}{x}\right)\right)$$

$$= \log x \sum_{d \leq x} \frac{\chi(d)}{d} - \sum_{d \leq x} \log d \frac{\chi(d)}{d} + C \sum_{d \leq x} \frac{\chi(d)}{d} + O\left(\frac{1}{x} \sum_{d \leq x} |\chi(d)|\right)$$

$$= \log x(L(1,\chi)) + O\left(\frac{1}{x}\right) + (K + O\left(\frac{\log x}{x}\right) + C(L(1,\chi)) + O\left(\frac{1}{x}\right) + O\left(\frac{1}{x} \cdot x\right)$$

$$= \log x(L(1,\chi) + O(1)$$

Chapter 7

proof by contradiction

Prove infinite number of primes of the form 4n-1.

Suppose there are finite number of primes of the form $4n-1$, that is $p_1..p_k$
Let $N = 4(p_1...p_k) - 1$.
N cannot be prime as $N > p_k$ so N must be a composite of primes in the form 4n+1.
But $(4n_1+1)(4n_2+1) = 16n_1n_2+4n_1+4n_2+1 = 4(4n_1n_2+n_1+n_2)+1 = 4n+1$ so it cannot be in this form, so must be in the form $4n-1$. This is a contradiction

8 Lemma 7.4

$$\sum_{\substack{p\leq x\\ p\equiv h \pmod k}} \frac{\log p}{p} = \frac{1}{\phi(k)}\log x + \frac{1}{\phi(k)}\sum_{r=2}^{\phi(k)} \overline{\chi}_r(h) \sum_{p\leq x} \frac{\chi_r(p)\log p}{p} + O(1)$$

For instance $p \equiv 3 \pmod 4$, $\phi(k) = 2$, $\overline{\chi}_r(h) = \chi_2(3) = -1$

$$\sum_{\substack{p\leq x\\ p\equiv 3 \pmod 4}} \frac{\log p}{p} = \frac{1}{\phi(k)}\log x - \frac{1}{2}\sum_{p\leq x} \frac{\chi_2(p)\log p}{p} + O(1)$$

$p \equiv 2 \pmod 5$, $\phi(k) = 4$, multiple $\overline{\chi}_r$

$$\sum_{\substack{p\leq x\\ p\equiv 2 \pmod 5}} \frac{\log p}{p} = \frac{1}{4}\log x + \frac{1}{4}\sum_{r=2}^{4} \overline{\chi}_r(2) \sum_{p\leq x} \frac{\chi_r(p)\log p}{p} + O(1)$$

9 Lemma 7.5

$$\sum_{p\leq x} \frac{\chi(p)\log p}{p} = -L'(1,\chi)\sum_{n\leq x} \frac{\mu(n)\chi(n)}{n} + O(1)$$

when χ is the nonprincipal character mod 4
LHS $\chi_2(1) = 1$, $\chi_2(3) = -1$ so we split up the formula

$$\sum_{p\leq x} \frac{\chi(p)\log p}{p} = \sum_{\substack{p\leq x\\ p\equiv 1 \pmod 4}} \frac{\log p}{p} - \sum_{\substack{p\leq x\\ p\equiv 3 \pmod 4}} \frac{\log p}{p}$$

For the 1st part f the RHS

$$L(1,\chi) = -\sum_{n=1}^{\infty} \frac{\chi(n)\log(n)}{n}$$

expanding we have $n = 1, 2, 3, ...$ (mod 4) where $\chi(2) = \chi(4) = 0$, $\chi(1) = 1$ and $\chi(3) = -1$, and $\log(1) = 0$ gives

$$-\left(-\frac{\log(3)}{3} + \frac{\log(5)}{5} - \frac{\log(7)}{7} + ...\right)$$

For the second part of the RHS, we can again split up the summation for $\chi_2(1) = 1$ and $\chi_2(3) = -1$

$$\sum_{n\leq x} \frac{\mu(n)\chi(n)}{n} = \sum_{\substack{n\leq x \\ p\equiv 1 \pmod 4}} \frac{\mu(n)}{n} - \sum_{\substack{n\leq x \\ p\equiv 3 \pmod 4}} \frac{\mu(n)}{n}$$

Thus

$$\sum_{\substack{p\leq x \\ p\equiv 1 \pmod 4}} \frac{\log p}{p} - \sum_{\substack{p\leq x \\ p\equiv 3 \pmod 4}} \frac{\log p}{p}$$

$$= \left(-\frac{\log(3)}{3} + \frac{\log(5)}{5} - \frac{\log(7)}{7} + ...\right)\left(\sum_{\substack{n\leq x \\ p\equiv 1 \pmod 4}} \frac{\mu(n)}{n} - \sum_{\substack{n\leq x \\ p\equiv 3 \pmod 4}} \frac{\mu(n)}{n}\right) + O(1)$$

(13)

$$\sum_{n\leq x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{d\leq x} \frac{\mu(d)\chi(d)}{d} \sum_{c\leq x/d} \frac{\chi(c)\log c}{c}$$

where $n = cd$

Non principle characters (mod 6) where $x = 10$
LHS

$$\sum_{n\leq 10} \frac{\chi(n)\Lambda(n)}{n} = \frac{\log(1)}{1} - \frac{\log(5)}{5} + \frac{\log(7)}{7} = -\frac{\log(5)}{5} + \frac{\log(7)}{7}$$

RHS, Breaking up the $\sum_{d\leq x}$, $n = cd \leq 10$ so $d = 1, 2, .., 10$ with $\chi(2) = \chi(3) = \chi(4) = \chi(6) = \chi(8) = \chi(9) = \chi(10) = 0$

Setting $d = 1$

$$\frac{\mu(1)\chi(1)}{1} \sum_{c\leq 10} \frac{\chi(c)\log c}{c} = 1\left(-\frac{log(5)}{5} + \frac{\log(7)}{7}\right) = -\frac{log(5)}{5} + \frac{\log(7)}{7}$$

setting $d = 5$

$$\frac{\mu(5)\chi(5)}{5}\sum_{c\leq 2}\frac{\chi(c)\log c}{c} = \log(1) = 0$$

setting $d = 7$

$$\frac{\mu(7)\chi(7)}{7}\sum_{c\leq 10/7}\frac{\chi(c)\log c}{c} = \log(1) = 0$$

Thus

$$-\frac{\log(5)}{5} + \frac{\log(7)}{7} = -\frac{\log(5)}{5} + \frac{\log(7)}{7}$$

If $\Lambda_1(n) = \log(n)$ when n is prime, then.

$$\sum_{n\leq x}\frac{\chi(n)\Lambda(n)}{n} = \sum_{p\leq x}\frac{\chi(p)\log p}{p}$$

10 Examples

Prove that

$$g(x) = f(x)\log x - \int_2^x t^{-1}f(t)$$

where

$$f(x) = \sum_{\substack{p\leq x\\ p\equiv 3 \pmod{10}}} 1 \qquad g(x) = \sum_{\substack{p\leq x\\ p\equiv 3 \pmod{10}}} \log p$$

Using Abel's Identity with $A(n) = f(n)$ and $h(n) = \log n$ we have

$$\begin{aligned} g(x) &= \sum_{\substack{p\leq x\\ p\equiv 3 \pmod{10}}} \log p \cdot f(n) \\ &= f(x)\log x - f(2)\log 2 - \int_2^x t^{-1}f(t)dt \\ &= f(x)\log x - \int_2^x t^{-1}f(t)dt \end{aligned}$$

Using the above, if $f(x) \sim \frac{1}{4}\pi(x)$ prove that $g(x) \sim \frac{1}{4}x$ With $\pi(x) = \frac{x}{\log x}$ we will need to divide through by x to give

$$\frac{g(x)}{x} = f(x)\frac{\log x}{x} - \frac{1}{x}\int_2^x t^{-1}f(t)dt$$

Now $f(x) \sim \frac{1}{4}\pi(x) \sim \frac{1}{4}\frac{x}{\log x}$ gives

$$\begin{aligned}\frac{g(x)}{x} &= \lim_{x\to\infty} \frac{1}{4}\frac{x}{\log x}\frac{\log x}{x} - \frac{1}{x}\int_2^x t^{-1}f(t)dt \\ &= \lim_{x\to\infty} \frac{1}{4} - \frac{1}{x}\int_2^x t^{-1}f(t)dt\end{aligned}$$

With $f(t) \sim \frac{1}{4}\pi(t) \sim \frac{1}{4}\frac{t}{\log t}$

$$\frac{f(t)}{t} = O\left(\frac{1}{\log t}\right)$$

Giving

$$\frac{g(x)}{x} = \lim_{x\to\infty} \frac{1}{4} - O\left(\frac{1}{x}\int_2^x \frac{1}{\log t}dt\right)$$

Splitting the integral

$$\begin{aligned}O\left(\frac{1}{x}\int_2^x \frac{1}{\log t}dt\right) &= O\left(\frac{1}{x}\int_2^{\sqrt{x}} \frac{1}{\log t}dt\right) + O\left(\frac{1}{x}\int_{\sqrt{x}}^x \frac{1}{\log t}dt\right) \\ &\leq O\left(\frac{1}{x}\left(\frac{\sqrt{x}}{\log 2} + \frac{x}{\log\sqrt{x}}\right)\right) \\ &\leq O\left(\frac{1}{\sqrt{x}\log 2} + \frac{1}{\log\sqrt{x}}\right)\end{aligned}$$

which tends to 0 as $x \to \infty$. Giving

$$\begin{aligned}\lim_{x\to\infty} \frac{g(x)}{x} &= \frac{1}{4} \\ \lim_{x\to\infty} g(x) &= \frac{1}{4}x \\ g(x) &\sim \frac{1}{4}x\end{aligned}$$

paragraph*Chapter 9

9 - Quadratic residues and the quadratic reciprocity law This chapter deals with the quadratic form $x^2 \equiv n \pmod{p}$

In theorems 5.28 and 5.30 we can see how $f(x) \equiv 0 \pmod{m}$ can be replaced by $f(x) \equiv 0 \pmod{p}$ Using the form

$$ax^2 + bx + c \equiv 0 \pmod{p} \quad \text{where } a \not\equiv 0 \pmod{p}$$

multiplying the formula by the number $4a$ which is relatively prime to p we get:

$$\begin{aligned} 4a^2x^2 + 4abx + 4ac &\equiv 0 \pmod{p} \\ 4a^2x^2 + 4abx + b^2 &\equiv b^2 - 4ac \pmod{p} \\ (2ax + b)^2 &\equiv b^2 - 4ac \pmod{p} \\ X^2 &\equiv n \pmod{p} \end{aligned}$$

where $X = 2ax + b$ and $n = b^2 - 4ac$

Before going any further we need to look at residue and non-residue meanings. If we have an odd number p, taking every integer $< p$ and squaring them, we get a set of numbers $\pmod{p}$. These are residue to p, the set of numbers that do not appear and non-residue to p For instance $p = 5$

x		1	2	3	4
x^2		1	4	9	16
X^2	$\pmod{5}$	1	4	4	1

Thus $\{1, 4\}$ are residual (denoted as R)to 5 and $\{2, 3\}$ are non residual (denoted as $\bar{R}$) to 5

We say that if the congruence has a solution then n is a quadratic residue $\pmod{p}$, that is nRp. If it as no solution then n is a quadratic non-residue $\pmod{p}$, that is $n\bar{R}p$

For there to be a solution to $X^2 \equiv n \pmod{p}$ n must be residual to p
Note that $1 \equiv -4 \pmod{5}$ thus $1^2 \equiv -4^2 \equiv 4^2 \pmod{5}$ therefore we do not have to check each value, but only in the range

$$1^2, 2^2 ... \left(\frac{p-1}{2}\right)^2$$

To see how this works, here is an example.
Reduce the congruence $3x^2 + 4x + 5 \equiv 0 \pmod{7}$. Does the congruence have any solutions?

We want to have the form $4a^2x^2+4abx...$ thus we must multiply the congruence by $4a = 12$ giving

$$36x^2 + 48x + 60 \equiv 0 \pmod 7$$

going through the motions.. we get down to $X = 2ax + b = 6x + 4$ and $n = b^2 - 4ac = 16 - 60 = -44$ Thus

$$X^2 = -44 \equiv 5 \pmod 7$$

checking the residues for $p = 7$

x		1	2	3
	x^2	1	4	9
X^2	(mod 5)	1	4	2

we see that 5 is non residue to (mod 7) so there are no solutions.

On a side note, if we were to find all the values of X which has solutions to 4 (mod 7) we see from the table above that this would be 2, and of course $-2 = 5$

Legendre's symbol and properties

9.2 Let p be an odd prime, if $n \not\equiv 0 \pmod p$ we define Legendre's symbol $(n|p)$ as

$$(n|p) = \begin{cases} +1, & \text{if } nRp. \\ -1, & \text{if } n\bar{R}p \end{cases}$$

If $n \equiv 0 \pmod p$ we define $(n|p) = 0$
Eaxamples

$(1|p) = 1$

$(\mathbf{m^2}|\mathbf{p}) = \mathbf{1}$ as it is a perfect square, and as seen in the tables above is a quadratic residue.

$(7|11) = -1$

$(22|11) = 0$

$(n|p)$ is a completely multiplicative function of n. That is if $p|m$ or $p|n$ then $p|mn$ so $(mn|p) = 0$.
If $p \not| m$ and $p \not| n$ then $p \not| mn$ and we have $(mn|p) \equiv (m|p)(n|p) \pmod p$

Eulers criterion states that let p be an odd prime, then for all n we have

$$(n|p) \equiv n^{(p-1)/2} \pmod p$$

For $p = 7$ we have

$$(n|7) \equiv n^3 \pmod 7$$

$$
\begin{aligned}
1^3 &\equiv 1 \pmod 7 \\
2^3 &\equiv 1 \pmod 7 \\
3^3 &\equiv -1 \pmod 7 \\
4^3 &\equiv 1 \pmod 7 \\
5^3 &\equiv -1 \pmod 7 \\
6^3 &\equiv -1 \pmod 7
\end{aligned}
$$

thus $nRp = \{1, 2, 4\}$ and $n\bar{R}p = \{3, 5, 6\}$ which agrees with the table for $p = 7$ above.

Using Eulers Criterion

$$(n|p) \equiv n^{(p-1)/2} \pmod p$$

With $(-1|p)$ we have

$$(-1|p) \equiv -1^{(p-1)/2} \pmod p = \begin{cases} +1, & \text{if } p \equiv 1 \pmod 4. \\ -1, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

and

$$(2|p) \equiv -1^{(p^2-1)/8} \pmod p = \begin{cases} +1, & \text{if } p \equiv \pm 1 \pmod 8. \\ -1, & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

Some examples

$$(4|11) = (2|11)^2 \text{ with } (2|p) = -1 \text{ as } 11 \equiv 3 \pmod 8 = -1^2 = 1$$

$$(-1|19) = -1 \text{ as } 19 \equiv 3 \pmod 4$$

$$(-10|13) = (-1|13)(2|13)(5|13) = (1)(-1)(-1) = 1$$

Which Dirichlet character is corresponding to the quadratic character $\pmod 5$
With $p = 5$ we have $nRp = \{1, 4\} = 1$ and $nP\bar{R}p = \{1, 4\} = -1$.
With $p = k = 5$ we have the table

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	**1**	**−1**	**−1**	**1**	**0**
$\chi_3(n)$	1	i	$-i$	-1	0
$\chi_4(n)$	1	$-i$	i	-1	0

Thus $\chi_2(n)$ is the corresponding dirichlet character to the quadratic character $\pmod 5$

Write out the proof of Theorem 9.5 in the case $p = 11$.

$$\begin{aligned} 10 \equiv & 1(-1)^1 \pmod{11} \\ 2 \equiv & 2(-1)^2 \pmod{11} \\ 8 \equiv & 3(-1)^3 \pmod{11} \\ 4 \equiv & 4(-1)^4 \pmod{11} \\ 6 \equiv & 5(-1)^5 \pmod{11} \end{aligned}$$

For the LHS we have $2 \cdot 4 \cdot 6 \cdot 8$ and the RHS we have $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot (-1)^{1+2+3+4+5}$, Thus

$$\begin{aligned} 2 \cdot 4 \cdot 6 \cdot 8 \equiv & 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot (-1)^{1+2+3+4+5} \\ 2^5 5! \equiv & 5!(-1)^{15} \\ 2^5 \equiv & -1^{15} \\ 2^5 \equiv & -1 \end{aligned}$$

Using Eulers criterion $(2|11) = -1$ as $11 \equiv 3 \pmod{8}$
Thus $(-1)^5 \equiv -1$

Guass' Lemma

Assume that $n \not\equiv 0 \pmod{p}$ and consider the least positive residuals $\pmod{p}$ of the $(p-1)/2$ multiples of n

$$n, 2n, 3n..., \frac{p-1}{2}n$$

If m denotes the number of residues which exceed $p/2$ then:

$$(n|p) = (-1)^m$$

Example:
Say we are to find $(11|19)$. Following above we the have$(19-1)/2 = 9$ values:

$$11, 22, 33, 44, 55, 66, 77, 88, 99 \equiv 11, 3, 14, 6, 17, 9, 1, 12, 4 \pmod{19}$$

With $p/2 = 19/2 = 9.5$ we have $m = 4$ so $(11|19) = (-1)^4 = 1$

Proof: Using $(11|19)$ we can split the least positive residues into 2 groups $A < p/2$ and $B > p/2$

$$\begin{aligned} A = & \{1, 3, 4, 6, 9\} \\ B = & \{11, 12, 14, 17\} \end{aligned}$$

We can also create a set C which is the values $C = p - B$

$$C = \{19-17, 19-14, 19-12, 19-11\} = \{2, 5, 7, 8\}$$

Multiplying everything in $A \cup C$, that is A union C which is everything in the sets A and C.

$$\begin{aligned}
1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 =& 1 \cdot 3 \cdot 4 \cdot 6 \cdot 9 \cdot (19-17) \cdot (19-14) \cdot (19-12) \cdot (19-11) \\
9! =& 1 \cdot 3 \cdot 4 \cdot 6 \cdot 9 \cdot (0-17) \cdot (0-14) \cdot (0-12) \cdot (0-11) \\
9! \equiv& (-1)^4 \cdot 1 \cdot 3 \cdot 4 \cdot 6 \cdot 9 \cdot 11 \cdot 12 \cdot 14 \cdot 17 \pmod{19}
\end{aligned}$$

Realising that The RHS are the least positive residuals (11|19) we can say

$$\begin{aligned}
9! \equiv& (-1)^4 \cdot 11 \cdot 22 \cdot 33 \cdot 44 \cdot 55 \cdot 66 \cdot 77 \cdot 88 \cdot 99 \pmod{19} \\
9! \equiv& (-1)^4 \cdot 11 \cdot 2(11) \cdot 3(11) \cdot 4(11) \cdot 5(11) \cdot 6(11) \cdot 7(11) \cdot 8(11) \cdot 9(11) \pmod{19} \\
9! \equiv& (-1)^4 \cdot 11^9 \cdot 9! \pmod{19} \\
11^9 \equiv& (-1)^4 \pmod{19} \\
n^{\frac{p-1}{2}} \equiv& (-1)^m \pmod{19}
\end{aligned}$$

Theorem 9.7

With large values the above can be very time consuming. As we have $(n|p) = (-1)^m$, all we need to know is if m is even or odd. Below will not work out the exact value for m just whether it is even or odd.
Let m be defined as above then:

$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right] + (n-1)\frac{p^2-1}{8} \pmod{2}$$

In Particular, if n is odd then:

$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right] \pmod{2}$$

For instance (11|19) we have:

$$\begin{aligned}
m \equiv& \sum_{t=1}^{(19-1)/2=9} \left[\frac{t11}{19}\right] + (11-1)\frac{19^2-1}{8} \pmod{2} \\
m \equiv& \left[\frac{11}{19}\right] + \left[\frac{22}{19}\right] + \left[\frac{33}{19}\right] + \left[\frac{44}{19}\right] + \left[\frac{55}{19}\right] + \left[\frac{66}{19}\right] + \left[\frac{77}{19}\right] + \left[\frac{88}{19}\right] + \left[\frac{99}{19}\right] + (10)\frac{19^2-1}{8} \pmod{2} \\
m \equiv& 0+1+1+2+2+3+4+4+5+0 \pmod{2} \\
m \equiv& 22 \equiv 0 \pmod{2}
\end{aligned}$$

Thus $(n|p) = (-1)^m = (-1)^0 = 1$

Reciprocity Law

If q and p are distinct odd primes then

$$(p|q)(q|p) = (-1)^{(p-1)(q-1)/4}$$

The quadratic reciprocity law above states that if if p and q are odd primes then $(p|q) = (q|p)$ unless $p \equiv q \equiv 3 \pmod 4$, in which case $(p|q) = -(q|p)$

Examples using this law:

Determine if 219 is quadratic reside or non-residue of $\pmod{383}$

We have $219 = 3 \cdot 73$ so we have $(219|383) = (3|383)(73|383)$
Starting with $(3|383)$, $3 \equiv 383 \equiv 3 \pmod 4$ so $(3|383) = -(383|3)$. Which gives $-383 \equiv -2 \pmod 3$ or $-(2|3) = (1|3) = 1$

For $(73|383)$, $73 \equiv 1 \pmod 4$ so we have $(73|383) = (383|73) = (18|73)$.
But $18 = 2 \cdot 9$ and as 9 is a perfect square $(9|73) = 1$ thus $(18|73) = (1)(2|73)$.
With $(2|73)$ as $73 \equiv 1 \pmod 8$, $(2|73) = 1$

Thus $(219|383) = 1 \cdot 1 = 1$ thus 219 is a quadratic residue $\pmod{383}$

The Jacobi Symbol To determine if a composite number is a quadratic reside or nonresidue $\pmod p$

If p is a positive odd integer with prime factorisation

$$P = \prod_{i=1}^{r} p_i^{a_i}$$

the Jacobi symbol $(n|P)$ is defined for all integers n by the equation

$$(n|P) = \prod_{i=1}^{r} (n|P_i)^{a_i}$$

where $(n|p_i)$ is the Legendre symbol. We also define $(n|1) = 1$

the possible values for $(n|P)$ are 1, -1, 0, with $(n|P) = 0$ iff $(n, P) > 1$

If the congruence

$$x^2 \equiv n \pmod P$$

has a solution then $(n|p_i) = 1$ for each prime p_i and hence $(n|P) = 1$. the converse is not true i,e $(n|P)$ can equal 1 if an even number of factors -1 appear in the 2nd equation.

Th9.9 If P and Q are odd positive integers, we have

$$\begin{aligned}(m|P)(n|P) =&(mn|P)\\ (n|P)(n|Q) =&(n|PQ)\\ (m|P) =&(n|P) \text{ whenever } m \equiv n \pmod{P}\\ (a^2n|P) =&(n|P) whenever (a, P) = 1\end{aligned}$$

Proof for $(n|P)(n|Q) = (n|PQ)$:
With $P = \prod_{i=1}^{r} p_i^{a_i}$ and $Q = \prod_{i=1}^{r} p_i^{b_i}$

$$(n|P)(n|Q) = \prod_{i=1}^{r}(n|p_i)^{a_i} \prod_{i=1}^{r}(n|p_i)^{b_i} = \prod_{i=1}^{r}(n|p_i^{a_i}p_i^{b_i}) = (n|PQ)$$

The special formulas for evaluating Legendre symbols $(-1|p)$ and $(2|p)$ also hold for the Jacobi symbol

Th9.10 If P is an odd positive integer we have

$$(-1|P) = (-1)^{(P-1)/2}$$

and

$$(2|P) = (-1)^{(P^2-1)/8}$$

Th9.11 Reciprocity Law - If P and Q are positive odd integers with $(P, Q) = 1$ then

$$(P|Q)(Q|P) = (-1)^{(P-1)(Q-1)/4}$$

Diophantine Equation

$$y^2 = x^3 + k$$

has no solutions if k has the form

$$k = (4n - 1)^3 - 4m^2$$

where m and n are integers such that no prime $p \equiv -1 \pmod 4$ divides m
First of we assume that x and y exists and obtain a proof by contradiction. Considering the equation $\pmod 4$, $k = (4n - 1)^3 - 4m^2 \equiv -1 \pmod 4$ so we have

$$y^2 \equiv x^3 - 1 \pmod 4$$

Now looking at y

$$\begin{aligned}y =&0, y^2 = 0 \pmod 4\\ y =&1, y^2 = 1 \pmod 4\\ y =&2, y^2 = 0 \pmod 4\\ y =&3, y^2 = 1 \pmod 4\end{aligned}$$

Therefore $y^2 \equiv 0$ or $1 \pmod 4$
With $x^3 = x^2x$ if x is even then we have $y^2 \equiv 0 - 1 \equiv -1 \pmod 4$, and the same that if $x \equiv -1 \pmod 4$ so we are left with $x \equiv 1 \pmod 4$
Now let $a = 4n - 1 \equiv -1 \pmod 4$ so that $k = a^3 - 4m^2$

$$\begin{aligned} y^2 \equiv & x^3 + a^3 - 4m^2 \pmod 4 \\ y^2 + 4m^2 \equiv & x^3 + a^3 \pmod 4 \\ y^2 + 4m^2 \equiv & (x + a)(x^2 - ax + a^2) \pmod 4 \end{aligned}$$

With $x \equiv 1$ and $a \equiv -1$ then looking at the RHS bracket we have $1 + a + a^2 = 3 \equiv -1 \pmod 4$
Therefore $x^2 - ax + a^2$ is odd and has some prime $p \equiv -1 \pmod 4$ it is divisible by. In other words

$$y^2 \equiv -4m^2 \pmod p$$

for some $p \equiv -1 \pmod 4$. but at the start we said that $p \not| m$ so with $(-4m^2|p) = (-1|p) = -1$ this contradicts the sentence above, proving that the Diophantine equation has no solutions when $k = (4n - 1)^3 - 4m^2$

Example Prove that

$$(-3)|p) = 1 \text{ if } p \equiv 1 \pmod 6 \text{ and } (-3|p) = 1 \text{ if } p \equiv 5 \pmod 6$$

with

$$(-1|p) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

$$(3|p) = \begin{cases} 1, & \text{if } p \equiv 1 \text{ or } 11 \pmod{12} \\ -1, & \text{if } p \equiv 5 \text{ or } 7 \pmod{12} \end{cases}$$

and by considering the number $4p_1^2p_2^2...p_n^2 + 3$ prove that there are infinitely many primes of the form $6k + 1$.

We have

$$(-3|p) = (-1|p)(3|p) = 1$$

Giving

$$((-1|p) = (3|p) = 1 \text{ or } (-1|p) = (3|p) = -1$$

For the 1st case we have

$$p \equiv 1 \pmod 4 \text{ and } (p \equiv 1 \text{ or } 11 \pmod{12})$$

thus

$$p \equiv 1 \pmod{12}$$

For the 2nd case

$$p \equiv 3 \equiv \pmod 4 \text{ and } (p \equiv 5 \text{ or } 7 \pmod{12})$$

thus

$$p \equiv 7 \pmod{12}$$

so, in either case

$$p \equiv 1 \pmod 6$$

The next part, we have

$$(-3|p) = (-1|p)(3|p) = -1$$

Giving

$$((-1|p) = 1, (3|p) = -1 \text{ or } (-1|p) = -1, (3|p) = 1$$

For the 1st case we have

$$p \equiv 1 \pmod 4 \text{ and } (p \equiv 5 \text{ or } 7 \pmod{12})$$

thus

$$p \equiv 5 \pmod{12}$$

For the 2nd case

$$p \equiv 3 \equiv \pmod 4 \text{ and } (p \equiv 1 \text{ or } 11 \pmod{12})$$

thus

$$p \equiv 11 \pmod{12}$$

so, in either case

$$p \equiv -1 \equiv 5 \pmod 6$$

For the last part. $N = 4p_1^2p_2^2...p_n^2 + 3$ cannot be prime therefore is a composite, thus we have

$$(2p_1p_2...p_n)^2 \equiv -3 \pmod 6$$

For which

$$(-3|p) = 1 \text{ when } p \equiv 1 \pmod 6$$

so

$$(p_i|(2p_1p_2..p_n)^2) \text{ for } i = 1, 2...n$$

With $N = (2p_1p_2..p_n)^2 + 3$, $(p_i|3)$ but with $p \equiv 1 \pmod 6$ this is impossible and therefore a contradiction. Thus there are infinite many primes of the form $6k + 1$