Number Theory Notes
8th December 2021

1 Jacobi Symbol

Jacobi extended the Legendre symbol to include $\left(\frac{a}{b}\right)$ when b is any odd positive number and a is any integer. If $b = p_1 p_2 \cdots p_r$ with odd primes p_i (not necessarily distinct) the definition is

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right).$$

This is convenient because the statements of QRL carry over to give the following:

Observation.
For odd numbers $r_1, \cdots, r_k$, we have:
$\sum_i (r_i - 1)/2 \equiv (r_1 \cdots r_k - 1)/2 \bmod 2$;
$\sum_i (r_i^2 - 1)/8 \equiv (r_1^2 \cdots r_k^2 - 1)/8 \bmod 2$.
To see this, write $r_i = 2s_i + 1$; then

$$r_1 r_2 \cdots r_k = \prod_{i=1}^{k} (2s_i + 1) \equiv 1 + 2\sum_i s_i \mod 4.$$

So,

$$r_1 r_2 \cdots r_k - 1 - \sum_i (r_i - 1) \equiv 0 \mod 4.$$

For the second observation, write $r_i^2 = 8t_i + 1$; then

$$r_1^2 r_2^2 \cdots r_k^2 = \prod_{i=1}^{k} (8t_i + 1) \equiv 1 + 8\sum_i v_i \mod 64.$$

Hence,

$$r_1^2 \cdots r_k^2 - 1 - (r_1^2 - 1) - \cdots - (r_k^2 - 1) \equiv 0 \mod 64.$$

Corollary of QRL. Let $b = p_1 \cdots p_r$ where p_i's are (not necessarily distinct) odd primes. Then,

(i) $\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2}$;

(ii) $\left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8}$;

(iii) if a is odd, $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{(a-1)(b-1)/4}$.

The proof is immediate from QRL and the observations on parity.

1.1 Quadratic non-residues

If a is a positive integer that is a perfect square modulo all (or all but finitely many) primes p, then is it true that it must be a perfect square? This is like a local-global property. Surprisingly, the answer is not immediate but it is yes, and requires QRL. It is convenient to use Jacobi symbols. The result is:

Let a be a non-square positive integer. Then, there are infinitely many primes p for which $\left(\frac{a}{p}\right) = -1$.

To prove this, we may assume a is square-free.

If $a = 2$, this is equivalent by QRL to showing that there are infinitely many primes of the form ± 3 mod 8. If $p_1, p_2, \cdots, p_r$ are any set of primes of the form ± 3 mod 8, the number $8p_1p_2\cdots p_r + 3$ is divisible by some new prime of one of these forms because primes that are ± 1 mod 8 multiply to a number that is ± 1 modulo 8.

Assume $a \neq 2$; so, we write $a = 2^e p_1 p_2 \cdots p_r$ where $e = 0$ or 1 and p_i's are odd primes (and $r \geq 1$). Start with ANY finite set of odd primes $q_1, \cdots, q_s$ different from the p_i's. Fix a quadratic non-residue u mod p_1. To ensure that we obtain an odd positive integer which is a square modulo the q_j's and all the p_i's other than p_1 while being a non-square mod p_1, we simply solve the CRT problem

$$b \equiv 1 \mod 8p_2p_3\cdots p_r q_1 q_2 \cdots q_s;$$

$$b \equiv u \mod p_1.$$

The odd number $b = l_1 l_2 \cdots l_n$ say. Note that

$$\left(\frac{a}{b}\right) = \left(\frac{2^e}{b}\right)\prod_{i=2}^{r}\left(\frac{p_i}{b}\right)\left(\frac{p_1}{b}\right) = -1$$

by the properties of the Jacobi symbol.
By QRL,

$$-1 = \left(\frac{a}{b}\right) = \prod_{j=1}^{s} \left(\frac{a}{l_j}\right)$$

which means $\left(\frac{a}{l_i}\right) = -1$ for some i. As l_i divides b which is coprime to the q_j's, we have produced new prime mod which a is a non-square. This proves the assertion.

2 Problems on QRL

The following problems are from the exercises following section 3.2 of NZM.

Exercise 17, section 3.2. If $19a^2 \equiv b^2 \bmod 7$ for some integers a, b, we claim that this congruence must hold modulo 7^2.
Indeed, if $(7, a) = 1$, then we would have $19 \equiv (a^{-1}b)^2 \bmod 7$ which means $\left(\frac{19}{7}\right) = 1$. This is clearly checked to not hold. Hence $7|a$. Hence $7|b$ also. So, we have $19a^2 \equiv b^2 \bmod 7^2$.

Exercise 20, section 3.2. If x, y are integers, we shall show that $\frac{x^2-2}{2y^2+3}$ cannot be an integer.
Indeed, the denominator is an odd number which is either 3 or 5 mod 8. Hence, it must have some prime divisor $p \equiv \pm 3 \bmod 8$. But such a prime cannot divide the numerator as, otherwise, 2 would be a quadratic residue mod p.

Exercise 22, section 3.2. If p is an odd prime not dividing ab, we show that the number of solutions for x, y satisfying $ax^2 + by^2 \equiv 1 \bmod p$ is $p - \left(\frac{-ab}{p}\right)$.
For any solution x, y we have, mod p,

$$a^2x^2 \equiv a - aby^2 = (-ab)(y^2 - b^{-1}).$$

That is, $\left(\frac{-ab(y^2-b^{-1})}{p}\right) = 1$.
We have already counted the number of solutions (as y varies) earlier, and have the expression

$$\sum_{y=0}^{p-1} \left(1 + \left(\frac{-ab}{p}\right)\left(\frac{y^2 - b^{-1}}{p}\right)\right).$$

As we have shown earlier that $\sum_{y=0}^{p-1} \left(\frac{y^2-b^{-1}}{p}\right) = -1$ (since $-b^{-1}$ is coprime to p), we get the expression asserted.

Exercise 23, section 3.2. If a, b are positive integers, then we claim

$$\sum_{r=1}^{[a/2]} [rb/a] + \sum_{s=1}^{[b/2]} [sa/b] = [a/2][b/2] - [GCD(a, b)/2].$$

This is exactly similar to Eisenstein's proof of QRL we discussed that used counting lattice points excepting that we have two integers a, b that may not be primes.
Look at the line $ay = bx$ and we first look at all the lattice points (x, y) with $1 \leq x \leq a/2$ and $1 \leq y \leq b/2$. These are clearly $[a/2][b/2]$ in number. Among them exactly $[GCD(a, b)/2]$ lie on the line. The other lattice points we counted are either below or above the line. Clearly, these are the two sums on the LHS of our assertion.

.---

2.1 More Problems on QRL

Exercise. If p is a prime such that a is not a multiple of p, we show that the number of solutions mod p to the congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ is equal to $1 + \left(\frac{b^2-4ac}{p}\right)$.

Note the particular case that $x^2 \equiv d \bmod p$ has $1 + \left(\frac{d}{p}\right)$ solutions.
We may consider odd p as $p = 2$ can be easily checked. Now, since $(a, 4p) = 1$, we have modulo p,

$$ax^2 + bx + c \equiv 0 \Leftrightarrow 4a(ax^2 + bx + c) \equiv 0$$

$$\Leftrightarrow (2ax + b)^2 \equiv b^2 - 4ac.$$

Thus, there are no solutions if $b^2 - 4ac$ is not a square mod p and 2 solutions when it is a non-zero square, and exactly one solution when $b^2 - 4ac \equiv 0 \bmod p$.

Exercise. For a prime p, we claim that $\sum_{y=0}^{p-1} \left(\frac{y^2+a}{p}\right)$ equals $p - 1$ or -1 according as to whether p divides a or not.
We may assume p does not divide a; else, it is clear.
By the above exercise, the number of solutions of $x^2 \equiv y^2 + a \bmod p$ is $1+\left(\frac{y^2+a}{p}\right)$. Therefore, varying y also, it follows that the number of solutions in x, y of $x^2 - y^2 \equiv a \bmod p$ is

$$\sum_{y=0}^{p-1} \left(1 + \left(\frac{y^2 + a}{p}\right)\right) = p + \sum_{y=0}^{p-1} \left(\frac{y^2 + a}{p}\right).$$

On the other hand, the number of solutions of $x^2 - y^2 \equiv a$ is exactly $p-1$ since this congruence is equivalent to $uv \equiv a$ where $u = x+y, v = x-y$, and since $(a,p) = 1$, each $v \neq 0$ has exactly one u. Comparison of the two expressions for the number of solutions proves $\sum_{y=0}^{p-1} \left(\frac{y^2+a}{p}\right)$ equals -1 when $(a,p) = 1$.

Exercise. We prove that every prime p dividing a number of the form $n^4 - n^2 + 1$ must be 1 mod 12.
Clearly, p must be odd first. Now, modulo p,

$$n^4 - n^2 + 1 \equiv 0 \;\Leftrightarrow\; 4n^4 - 4n^2 + 4 \equiv 0 \;\Leftrightarrow (2n^2-1)^2 \equiv -3.$$

So $\left(\frac{-3}{p}\right) = 1$. By QRL, this is equivalent to $\left(\frac{p}{3}\right) = 1$ which means $p \equiv 1$ mod 3.
Now, $n^4 \equiv n^2 - 1$ mod p implies $n^2 - 1$ is a square mod p. But,

$$-1 \equiv n^4 - n^2 = n^2(n^2-1)$$

which means -1 is a square mod p. Hence $p \equiv 1$ mod 4 also; we get $p \equiv 1$ mod 12.

Exercise. Let D be an odd, square-free, positive integer. We show there exists b such that $\left(\frac{D}{b}\right) = -1$.
Write $D = [_1 \cdots p_r$. Let u be a quadratic non-residue mod p_1. By CRT, choose an integer b satisfying

$$b \equiv 1 \;\; mod \;\; 4p_2 \cdots p_r;$$

$$b \equiv u \;\; mod \;\; p_1.$$

Clearly,

$$\left(\frac{b}{D}\right) = \prod_{i=1}^{r} \left(\frac{b}{p_i}\right) = -1$$

which gives $\left(\frac{D}{b}\right) = \left(\frac{b}{D}\right) = -1$.

Exercise*.
The purpose of this exercise is to prove that a prime p which is 1 mod 4, we have 2 to be a 4-th power modulo p, if and only if, p is expressible as $A^2 + 64B^2$.

Let $p \equiv 1 \bmod 4$ be a prime, and write $p = a^2 + b^2$ with a odd, say without loss of generality.

Claim I. $\left(\frac{a}{p}\right) = 1$.

This is because $p = a^2 + b^2 \equiv b^2 \bmod a$ which gives the Jacobi symbol $\left(\frac{p}{a}\right) = 1$. By QRL, we get $\left(\frac{a}{p}\right) = 1$.

Claim II. $\left(\frac{a+b}{p}\right) = (-1)^{((a+b)^2-1)/8}$.

Note that $a + b$ is odd and $p \equiv 1 \bmod 4$ which gives

$$\left(\frac{a+b}{p}\right) = \left(\frac{p}{a+b}\right).$$

Now $2p = (a+b)^2 + (a-b)^2 \equiv (a-b)^2 \bmod a+b$. Hence

$$\left(\frac{2p}{a+b}\right) = \left(\frac{2}{a+b}\right)\left(\frac{p}{a+b}\right) = 1.$$

Therefore,

$$\left(\frac{p}{a+b}\right) = \left(\frac{2}{a+b}\right) = (-1)^{((a+b)^2-1)/8}.$$

Claim III. $(a+b)^{(p-1)/2} \equiv (2ab)^{(p-1)/4}$.

This is immediate from $(a+b)^2 \equiv 2ab \bmod p$.

Claim IV. $2^{(p-1)/4} \equiv f^{ab/2}$ where $f^2 \equiv -1$.

Indeed, let $f = ba^{-1} \bmod b$, then $f^2 \equiv -1$ since $b^2 \equiv -a^2$.

Also, since the LHS's in claims II and III are the same modulo p, we get

$$(-1)^{((a+b)^2-1)/8} \equiv (2ab)^{(p-1)/4}.$$

LHS here is $f^{((a+b)^2-1)/4} = f^{(p-1)/4} f^{ab/2}$, and
the RHS is $2^{(p-1)/4} a^{(p-1)/2} f^{(p-1)/4}$ after putting $b \equiv af$.
Therefore, since $a^{(p-1)/2} \equiv 1 \bmod p$ by claim I, we get claim IV.
Finally, we note that 2 is a 4-th power mod p if, and only if, $2^{(p-1)/4} \equiv 1 \bmod p$. This is if, and only if, $f^{ab/2} \equiv 1 \bmod p$.
As $f^2 \equiv -1$, the above happens if and only if, 4 divides $ab/2$. As a is odd, this is equivalent to $8|b$. This completes the characterization that 2 is a 4-th power modulo a prime $p \equiv 1 \bmod 4$ if, and only if, $p = a^2 + 64B^2$.

2.2 Greatest Integer Function

The ubiquitous functions $x \mapsto \lfloor x \rfloor$ and $x \mapsto \lceil x \rceil$ from the set of real numbers to the set of integers are very useful in number theory. These are, respectively, the largest integer that is at the most x and the smallest integer that is at least x. The former is the one that occurs more often, and one often writes $[x]$ for it, and calls it informally 'the greatest integer function'. We will not have occasion to discuss $\lceil x \rceil$ at this point. The definition of $]x]$ is deceptively simple, its properties are very handy (for example, we have already seen it appear in some proofs of the quadratic reciprocity law), and there are many questions involving them that are difficult to answer. We put together some of its basic properties that are less obvious on a first look - these are left as easy exercises.

Some basic properties of $[x]$:

(i) $[x] + [y] \leq [x + y] \leq [x] + [y] + 1$.
(ii) $[x] + [-x] = -1$ if x is not an integer.
(iii) $-[-x] = \lceil x \rceil$.
(iv) $[x + 1/2]$ is the nearest integer to x where the nearest is the larger one in case of half-integers.
(v) $-[-x + 1/2]$ is the nearest integer to x where the nearest is the smaller one in case of half-integers.

de Polignac's formula. The power of a prime p dividing $n!$ (denoted $v_p(n!)$) equals the sum $\sum_{r \geq 1} [n/p^r]$.
Firstly, the note that the sum is a finite sum. The proof of the formula is easy - observe that $[n/a]$ counts the number of multiples of a from 1 to n; therefore, the summands $[n/p] + [n/p^2]$ count the multiples of p^2 once each etc.

As an immediate application, we can see that the multinomial coefficient $\frac{n!}{a_1!a_2!\cdots a_r!}$ (where $a_1 + \cdots + a_r = n$) is an integer - just observe that

$$\sum_{i=1}^{r} [a_i/p^k] \leq [(a_1 + \cdots + a_r)/p^k]$$

for all k.

2.2.1 A few problems/properties involving $[x]$

1. The power of 10 dividing $n!$ is $v_5(n!)$ for every n. In other words, we have a formula for the number of zeroes that $n!$ ends in.
This is obvious from de Polignac's formula because if 5^k and 2^l are the powers of 5 and 2 (respectively) dividing $n!$, then $k \leq l$.

2. *Show, for all $n \geq 1$, that*

$$[\sqrt{n} + \sqrt{n+1}] = [\sqrt{4n+1}] = [\sqrt{4n+2}] = \sqrt{4n+3}].$$

As $n < \sqrt{n(n+1)} < n+1$, we get

$$2n < 2\sqrt{(n(n+1)} = (\sqrt{n} + \sqrt{n+1})^2 - (2n+1) < 2(n+1).$$

Thus,

$$4n + 1 < (\sqrt{n} + \sqrt{n+1})^2 < 4n + 3.$$

Taking square roots,

$$\sqrt{4n+1} < \sqrt{n} + \sqrt{n+1} < \sqrt{4n+3}.$$

If $m = [\sqrt{4n+1}]$, we have $[\sqrt{4n+3}] < m+1$ because no perfect square can be either of the form $4n+2$ or of the form $4n+3$. Thus, we have the assertion.

5. For any positive integers $2 \leq d \leq n$, consider the base d expansion of n; say, $n = a_0 + a_1 d + \cdots + a_r d^r$ with $0 \leq a_i < d$. Then, for all $i \geq 0$,

$$a_i = [n/d^i] - d[n/d^{i+1}].$$

In particular, if $d = p$, a prime, the power of p dividing $n!$ equals $\frac{n - \sum_{i=0}^{r} a_i}{p-1}$.
Thus, we may determine the power of a prime dividing $n!$ in terms of the sum of the base p digits of n.
The assertion giving the values of a_i's is easy to see. For the second assertion when $d = p$, a prime, consider $n - \sum_{i \geq 0} a_i$ and feed the values of a_i from the first assertion. We obtain

$$n = \sum_i a_i = (p-1)([n/p] + [n/p^2] + \cdots + [n/p^r])$$

which gives the assertion using de Polignac's formula.

3 Arithmetic Functions

Some examples of arithmetic functions are $\mu(n), \phi(n), d(n), \sigma(n), \sigma_k(n), \omega(n), \Omega(n)$.
An arithmetic function f is *multiplicative* if it is not identically zero (equivalently $f(1) \neq 0$) and $f(mn) = f(m)f(n)$ for all $(m, n) = 1$.
The functions $\mu(n), \phi(n), d(n), \sigma(n), \sigma_k(n)$ are multiplicative. The proof is by induction on the number of prime divisors and depends on the observation that divisors of mp^r for $(m, p) = 1$ with p prime, are of the form dp^s with $d|m$ and $0 \leq s \leq r$.
We leave it for you to write out; we will give a general proof that includes all these cases.
The values of a multiplicative function are determined by the values at prime powers. For prime powers, we have:

$$\phi(p^r) = p^r(1 - 1/p);$$

$$d(p^r) = r + 1;$$

$$\sigma_k(p^r) = \frac{p^{k(r+1)} - 1}{p^k - 1};$$

The proof of multiplicativity A function f is completely multiplicative if it is not the zero function and $f(mn) = f(m)f(n)$ for all m, n.
The k-th power function $n \mapsto n^k$ is completely multiplicative.
The *Liouville function*

$$\lambda(\prod_{i=1}^{r} p_i^{a_i}) = (-1)^{a_1 + \cdots + a_r}$$

is completely multiplicative.

3.1 Dirichlet Convolution

Given arithmetic functions f, g we have a "convolution product" defined by

$$(f * g)(n) = \sum_{ab=n} f(a)g(b) = \sum_{d|n} f(d)g(n/d).$$

Combining with the natural addition $f + g$, we have a commutative ring A with unity. The multiplicative identity is the function $I(n) = \delta_{1,n}$; that is $f * I = f$ for all f.

We show now that every arithmetic function f with $f(1) \neq 0$ has a Dirichlet inverse. In fact, clearly we may define the inverse f^{-1} recursively by

$$f^{-1}(n) = -\frac{1}{f(1)} \sum_{d|n, d<n} f^{-1}(d) f(n/d).$$

Rephrasing in terms of Dirichlet series

We shall study later series of the form $\sum_{n\geq 1} \frac{f(n)}{n^s}$ in a complex variable and f is an arithmetic function. The convolution $f * g$ of arithmetic functions corresponds to the product of the corresponding series; that is,

$$F(s) := \sum_n \frac{f(n)}{n^s}, G(s) := \sum_n \frac{g(n)}{n^s}$$

give

$$F(s)G(s) := \sum_n \frac{(f*g)(n)}{n^s}.$$

The inclusion-exclusion principle.
By this title, we mean here the identity $\sum_{d|n} \mu(d) = I(n)$.
If $n = 1$, it is clear. Let $n > 1$ and write $n = \prod_{i=1}^r p_i^{a_i}$ where p_i's are distinct primes. The divisors of n are of the form $\prod_{j\in J} p_j^{b_j}$ where $J \subset \{1, 2, \cdots, r\}$ and $b_j \leq a_j$ for each j. Since μ vanishes on non-(square-free) numbers, the sum

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{i=1}^r \mu(p_i) + \sum_{i\neq j} \mu(p_i p_j) + \cdots + \mu(p_1 p_2 \cdots p_r)$$

$$= \binom{r}{0} - \binom{r}{1} + \binom{r}{2} - \cdots + \binom{r}{r}(-1)^r = (1-1)^r = 0 = I(n).$$

Later, we will see the above from a general result.