Dr. Marques Sophie
Office 519

Number theory

Spring Semester 2014
marques@cims.nyu.edu

Problem Set #1 with solution

Exercise 1 p 5 [N]:
$\alpha \in \mathbb{Z}[i]$ is unit if and only if $N(\alpha) = 1$.

Solution:
Suppose that α is a unit of $\mathbb{Z}[i]$ then there is $\gamma \in \mathbb{Z}[i]$ such the $\alpha\gamma = 1$, then $N(\alpha)|1$ and since $N(\alpha)$ is a positive integer then $N(\alpha) = 1$.
Suppose that $N(\alpha) = 1$ then $\alpha\bar{\alpha} = 1$ and $\bar{\alpha}$ is an inverse of α.
(Note that the units are precisely ± 1 and $\pm i$. Indeed, ± 1, $\pm i$ are clearly unit (and of norm 1). Let $a + ib \in \mathbb{Z}[i]$ of norm 1, then $a^2 + b^2 = 1$, but the only possibilities are that $a = \pm 1$ and $b = \pm i$, hence the result.)

Exercise 3 p 5 [N]:
Show that the integer solutions of the equation

$$x^2 + y^2 = z^2$$

such that $x, y, Z > 0$ and $(x, y, z) = 1$ ("pythagorean triple") are all given, up to possible permutation of x and y, by the formulae

$$x = u^2 - v^2,\ y = 2uv,\ z = u^2 + v^2,$$

where $u, v \in \mathbb{Z}$, $u > v > 0$, $(u, v) = 1$, u, v not both odd.

Solution:
Since if (x, y, z) is a Pythagorean triple, then $(\lambda x, \lambda y, \lambda z)$ is also a Pythagorean triple. It is also clear that all Pythagorean triples are multiples of the primitive ones. Hence to determine all Pythagorean triples it suffices to determine the primitive ones, i.e x, y and z are coprime.
First, notice that in a Pythagorean triplet a and b cannot be both odd. For then we would have $a^2 + b^2 \equiv 1 + 1 \equiv 2$ mod 4 but c^2, being a square, cannot be $\equiv 1$ mod 4 .

Claim 1: *Suppose (x, y, z) is a primitive Pythagorean triple. Then $x + yi$ and $x - yi$ are relatively prime in $\mathbb{Z}[i]$ i.e. they have no common prime divisors in $\mathbb{Z}[i]$.*
Proof of the claim: *Suppose instead $x + iy$ and $x - iy$ have a common prime divisor $\pi \in \mathbb{Z}[i]$. Then π divides their sum $2x$ and their difference $2yi$. Since x and y have*

no common fractors in $\mathbb{Z}$, they have no common prime factors in $\mathbb{Z}[i]$. Thus must be a prime dividing 2, i.e., $\pi = \pm 1 + \pm i$. Then

$$N(\pi) = \pi\bar{\pi} = 2|(x+yi)(x-yi) = x^2 + y^2 = z^2$$

This means z is even, so $x^2 + y^2 \equiv 0 \ mod\ 4$ which implies x and y are both even, a contradiction.

<u>Claim 2:</u> Suppose α, $\beta \in \mathbb{Z}[i]$ are relatively prime. If $\alpha\beta = \gamma^2$ is a square in $\mathbb{Z}[i]$, then $u\alpha$ and $u^{-1}\beta$ are squares for some unit u of $\mathbb{Z}[i]$.
Proof of the claim: *Note that this is trivial if γ is a unit (and vacuous if $\gamma = 0$). So assume $\alpha\beta$ is the square of some $\gamma \in \mathbb{Z}[i]$, where γ is a non-zero non-unit. Then γ has a prime factorization in $\mathbb{Z}[i]$:*

$$\gamma = \prod \pi_i^{e_i}$$

Thus the prime factorization of

$$\alpha\beta = \prod \pi_i^{2e_i}$$

up to a reordering of primes, since π_i and π_j are coprime if $i \neq j$, we have

$$\alpha = u^{-1}\pi_1^{2e_1}...\pi_j^{2e_j}$$

$$\beta = u\pi_{i+2}^{2e_j+1}...\pi_k^{2e_k}$$

for some unit u.
Solution of the initial problem ($\Leftarrow$) Suppose we have u and v with the given properties. Clearly a, b and c satisfied $a^2+b^2 = c^2$ and $gcd(a,c)$ divides $gcd(c-a, c+a) = gcr(2u^2, 2v^2) = 2$. But since $u \not\equiv v \ mod\ 2$, a and c are odd and so $gcd(a,c) = 1$. Hence, $gcd(a,b,c) = 1$.
($\Rightarrow$) Suppose (x,y,z) is a primitive Pythagorean triple, so $x^2+y^2 = (x+iy)(x-yi) = z^2$. By the first lemma, $x+iy$ and $x-iy$ are relatively prime, and by the second they are units times squares. In particular $x+iy = \pm\alpha^2$ or $x+yi = \pm i\alpha^2$ for $\alpha \in \mathbb{Z}[i]$. Since -1 is a square in $\mathbb{Z}[i]$, we may absorb the possible minus sign into α and write either $x+yi = \alpha^2$ or $x+iy = i\alpha^2$.
Write $\alpha = u+iv$, and we get in the first case

$$x+iy = (u+vi)^2 = u^2+v^2+2uvi$$

and

$$x+yi = i(u+vi)^2 = -2uv + (u^2+v^2)i$$

In the first case, we have $x = u^2+v^2$, $y = 2uv$. In the second, we may replace u by $-u$ or v by $-v$ to write $x = 2uv$, $y = u^2+v^2$ and to obtain u and v in $\mathbb{N}$. Then the conditions $gcd(u,v) = 1$, $u > v$ and u, v not both odd all follow from the facts that $gcd(x,y) = 1$ and $x, y > 0$.
The last statement is obvious.

Let d be a square free integer and $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\}$ be the subring of the quadratic extension $\mathbb{Q}[\sqrt{d}]$ of $\mathbb{Q}$. (Notice that it is not always equal to the ring of the integer of this quadratic extension (see Exercise 4 p 15)). Let N be the multiplicative map:

$$N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 + db^2 \in \mathbb{Z}$$

(Note that is it is the restriction to $\mathbb{Z}[\sqrt{d}]$ of norm map for the quadratic extension $\mathbb{Q}[\sqrt{d}]$ of $\mathbb{Q}$ since the Galois group of this quadratic extension is formed by the identity map and the map sending $a + \sqrt{d}b$ to $a - \sqrt{d}b$).
We show that $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ is a unit if and only if

- $a^2 - db^2 = 1$, if $d \leq 1$;
- $a^2 - db^2 = \pm 1$, if $d > 1$;

Indeed, let $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ be a unit, then there is $\beta \in \mathbb{Z}[\sqrt{d}]$ such that $\alpha\beta = 1$ so that by multiplicativity of N applied to the equality, we get $N(\alpha)N(\beta) = 1$ and,

- when $d \leq 1$, then $N(\alpha) = a^2 + (-d)b^2 \in \mathbb{N}$, this implies that $N(\alpha) = 1$ i.e. $a^2 - db^2 = 1$;
- when $d > 1$, then $N(\alpha) = a^2 - db^2 \in \mathbb{Z}$, this implies that $N(\alpha) = \pm 1$ i.e. $a^2 - db^2 = \pm 1$.

Now, let $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$

- if $d \leq 1$ and $a^2 - db^2 = 1$ then $\alpha(a - \sqrt{d}b) = 1$ with $\alpha = a - b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ so that α is a unit;
- if $d > 1$ and $a^2 - db^2 = \pm 1$, then $\alpha(\pm(a - \sqrt{d}b)) = 1$ with $\alpha = \pm(a - b\sqrt{d}) \in \mathbb{Z}[\sqrt{d}]$ so that α is also a unit.

Exercise 5 p 5 [N] :
Show that the only units of the ring $\mathbb{Z}[\sqrt{-d}] = \mathbb{Z} + \mathbb{Z}\sqrt{-d}$, for any rational integer $d > 1$ are ± 1.
Solution:
Let $\alpha = a + b\sqrt{-d}$ be a unit of $\mathbb{Z}[\sqrt{-d}]$ since $d > 1$, this is equivalent to $a^2 + db^2 = 1$, but since a and b are integers, this is equivalent to $b = 0$ and $a = \pm 1$.

We recall how to prove that a Pell's Fermat equation has infinitely many solution.
Claim 1: Let $N \in \mathbb{N}$ and suppose N is not a square. Then there exist $x \neq 1, y \neq 0 \in \mathbb{N}$ such that $x^2 - Ny^2 = 1$.
Proof of claim 1: For $N = 2, 3, 5, 6$ our theorem is true since we have $3^2 - 2 \times 2^2 = 1$, $2^2 - 3 \times 1^2 = 1$, $9^2 - 5 \times 4^2 = 1$, $5^2 - 6 \times 2^2 = 1$. So, we can assume that $N \geq 7$.
Consider the continued fraction expansion of $\sqrt{N}$ given by

$$\sqrt{N} = [a_0, \overline{a_1, ..., a_r, 2a_0}]$$

say. Let $p/q = [a_0, ..., a_r]$. Then, from our elementary estimates we find that

$$|\frac{p}{q} - \sqrt{N}| < \frac{1}{2a_0 q^2}$$

Multiply on both side by $|p/q + \sqrt{N}| \leq (2\sqrt{N}+1)$. We find,

$$|\frac{p^2}{q^2} - N| < \frac{2\sqrt{N}+1}{2a_0 q^2}$$

Multiply on both sides by q^2 to find $|p^2 - Nq^2| < (2\sqrt{N}+1)/2[\sqrt{N}]$. When $N \geq 7$ we have

$$\frac{2\sqrt{N}+1}{2[\sqrt{-N}]} < \frac{2\sqrt{N}+1}{2(\sqrt{N}-1)} < 2$$

Hence, $|p^2 - Nq^2| < 2$. So, we have either $p^2 - nq^2 = -1$ or $p^2 - Nq^2 = 1$. (why can't we have $p^2 - Nq^2 = 0$?). In case $p^2 - Nq^2 = 1$ we find $x = p$, $y = q$ as solution. In case $p^2 - Nq^2 = -1$ we notice that $(p^2 + Nq^2)^2 - N(2pq)^2 = (p^2 - Nq^2)^2 = 1$. Hence we have the solution $x = p^2 + Nq^2$, $y = 2pq$.

Once we get this non-trivial solution we get infinitely many solutions, by the following:
Claim 2: Choose the solution of Pell's equation with $x + y\sqrt{N} > 1$ and minimal. Call it (p, q). Then, to any solution $x, y \in \mathbb{N}$ of Pell's equation there exists $n \in \mathbb{N}$ such that $x + y\sqrt{N} = (p + q\sqrt{N})^n$.
Proof of claim 2: Notice that if $u, v \in \mathbb{Z}$ satisfy $u^2 - Nv^2 = 1$ and $u + v\sqrt{N} \geq 1$, then $u - v\sqrt{N}$, being equal to $(u + v\sqrt{N})^{-1}$ lies between 0 and 1. Addition of the inequalities $u + v\sqrt{N} \geq 1$ and $0 \leq u - v\sqrt{N} \leq 1$ implies $u \geq 0$. Substraction of these inequalities yields $v > 0$. We call $u + v\sqrt{N}$ the size of the solution u, v. Now, let $x, y \in \mathbb{N}$ be any solution of Pell's equation. Notice that $(x + y\sqrt{N})(p - q\sqrt{N}) = (px - qyN) + (py - qx)\sqrt{N}$. Let $u = px - qyN$, $v = py - qx$ an we have $u^2 - Nv^2 = 1$ and $u + v\sqrt{N} = (x + y\sqrt{N})/(p + q\sqrt{N})$. Observe that

$$1 \leq \frac{x + y\sqrt{N}}{p + q\sqrt{N}} < \frac{x + y\sqrt{N}}{2}$$

hence $1 \leq u + v\sqrt{N} < \frac{x+y\sqrt{N}}{2}$. So we have found a new solution with positive coordinates and size bounded by half the size of $x + y\sqrt{N}$. By repeatedly performing this operation we obtain a solution whose size is less than the size of $p + q\sqrt{N}$. By the minimality of p, q this implies that this last solution should be $1, 0$. Supposing the number of steps is n we thus find that $x + y\sqrt{N} = (p + q\sqrt{N})^n$.

Exercise 6 p 5 [N]:
Show that the ring $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d}$, for squarefree rational integer $d > 1$, has infinitely many units.

Solution:
Let $\alpha = a + b\sqrt{d}$ be a unit of $\mathbb{Z}[\sqrt{d}]$ since $d > 1$, this is equivalent to $a^2 - db^2 = \pm 1$, but already $a^2 - db^2 = 1$ is a Pell's equation that we have just seen to have infinitely many solutions. As a consequence, we have infinitely many units.

Exercise 7 p 5 [N]:
Show that the ring $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$ is euclidean. Show furthermore that its units are given by $\pm(1+\sqrt{2})^n$, $n \in \mathbb{Z}$ and determine its prime elements.

Solution:
Consider $x, y \in \mathbb{Z}[\sqrt{2}]$, so that $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$, for a, b, c, $d \in \mathbb{Z}$. We can calculate the quotient:

$$\begin{aligned} \tfrac{y}{x} &= \tfrac{a+b\sqrt{2}}{c+d\sqrt{2}} \\ &= \tfrac{a+b\sqrt{2}}{c+d\sqrt{2}} \cdot \tfrac{c-d\sqrt{2}}{c-d\sqrt{2}} \\ &= \tfrac{(ac-2bd)+(bc-ad)\sqrt{2}}{c^2-2d^2} \\ &= \left(\tfrac{ac-2bd}{c^2-2d^2}\right) + \left(\tfrac{bc-ad}{c^2-2d^2}\right)\sqrt{2} \end{aligned}$$

Let $f = \frac{ac-2bd}{c^2-2d^2} \in \mathbb{Q}$ and $g = \frac{bc-ad}{c^2-2d^2} \in \mathbb{Q}$ so that $y/x = f + g\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Let $q = u + v\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, where $u \in \mathbb{Z}$ is the closest integer to $g \in \mathbb{Q}$. This implies that $|f - u| \leq 1/2$ and $|g - v| \leq 1/2$. Consider the following:

$$\begin{aligned} N(y/x - q) &= N((f + g\sqrt{2}) - (u + v\sqrt{2})) \\ &= N((f-u) + (g-v)\sqrt{2}) \\ &= |(f-u)^2 - 2(g-v)^2| \\ &\leq (f-u)^2 + 2(g-v)^2 \\ &\leq (1/2)^2 + 2(1/2)^2 \\ &= 3/4 \end{aligned}$$

Define $r = y - qx \in \mathbb{Z}[\sqrt{2}]$ so that $y = qx + r$. Now, consider $N(r)$:

$$\begin{aligned} N(r) &= N(y - qx) \\ &= N(x(y/x - q)) \\ &= N(x)N(y/x - q) \text{ Since } N \text{ is multiplicative.} \\ &\leq N(x)(3/4) \\ &< N(x) \end{aligned}$$

Note: If $q = y/x$ then $y = qx$ and $r = 0$.
We have therefore proven that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean Domain.
We have seen that $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is a unit if and only if $a^2 - 2b^2 = \pm 1$. So that if $a \neq 0$, then $a^2 \geq 1$ so that $|b| \leq |a| < 2|b|$.
First, we notice that it is enough to consider the case when $a, b \geq 0$, indeed if a and b negative then we have that $a + b\sqrt{2} = -(-a - b\sqrt{2})$ with $-a$ and $-b$ positive. Now

if a *positive and* b *negative then* $\frac{1}{a-(-b)\sqrt{2}} = \frac{a+(-b)\sqrt{2}}{a^2-2b^2} = \pm(a+(-b)\sqrt{2})$ *with* a *and* $-b$ *positive and finally if* a *negative and* b *positive, then* $-(a+b\sqrt{2})$ *corresponds to the previous case.*
Let, now restrict ourselves to $a, b \geq 0$*, and prove that the units are of the form* $(1+\sqrt{2})^n$ *by induction on* b*, we prove that for any* $b \in \mathbb{N}$*, there is an integer* n *such that* $a+b\sqrt{2} = (1+\sqrt{2})^N$*.*
If $a, b > 0$ *and* $a+b\sqrt{2}$ *is a unit then*

$$(a+b\sqrt{2})(\sqrt{2}-1) = (2b-a)+(a-b)\sqrt{2}$$

is also a unit. Since we know that $b \leq a < 2b$*, we have that* $2b-a > 0$ *and* $0 \leq a-b < b$*, so by induction, there is an integer* n *such that:*

$$(a+b\sqrt{2})(\sqrt{2}-1) = (1+\sqrt{2})^n$$

But multiplying both sides by $1+\sqrt{2}$ *you get:*

$$a+b\sqrt{2} = (1+\sqrt{2})^{n+1}$$

As a consequence, we get the result we want by induction.

Now, we want to know all the prime of $\mathbb{Z}[\sqrt{2}]$. For this, let's make make some remarks which works in general good to know,

<u>*Claim:*</u> *If $\mathbb{Z}(\sqrt{d})$ has the unique factorization property (which is the case when the ring is Euclidean and then prime elements are exactly the irreducible element), then*

1. *If $\alpha \in \mathbb{Z}(\sqrt{d})$ and $N(\alpha)$ is a prime in $\mathbb{Z}$, then α is irreducible.*
2. *Any natural prime p is either a prime π or a product $\pi'\pi''$ of two (not necessarily distinct) primes of $\mathbb{Z}(\sqrt{d})$;*
3. *The totality of primes π, π' and π'', obtained by applying (2) to all the natural primes, together with their associates, constitute the set of all primes of $\mathbb{Z}(\sqrt{d})$.*
4. *An odd natural prime p not divisor of d is a product $\pi'\pi''$ of two prime if and only if d is a quadratic residue modulo p.*

Proof of the claim:

1. *Suppose that $\alpha \in \mathbb{Z}(\sqrt{d})$ and $N(\alpha)$ is a prime in $\mathbb{Z}$ and α not irreducible that is there is an element β and γ in $\mathbb{Z}(\sqrt{d})$ non-unit, i.e. with $|N(\beta)|$ and $|N(\gamma)|$ integer strictly greater to 1 such that $\beta\gamma = 1$ but applying the norm which is multiplicative to the equality we obtain $N(\alpha)N(\beta) = 1$ which is impossible.*
2. *A natural prime p is either a prime, π, of $\mathbb{Z}(\sqrt{d})$ or composite i.e. $p = \pi'\pi''$, where π' and π'' are non-unit integers of $\mathbb{Z}(\sqrt{d})$. In the latter case, $N(\pi')N(\pi'') = N(p) = p^2$. Since π' and π'' are not units, there norms are unequal to 1 , so that we must have $N(\pi') = N(\pi'') = p$. Hence, by (1), π' and π'' are primes.*
3. *First prove that any prime π of $\mathbb{Z}(\sqrt{d})$, there corresponds a unique natural prime p which is divisible by π. Indeed, a prime π of $\mathbb{Z}(\sqrt{d})$ is a divisor of its norm. Hence there exist natural divisible by π. Let n be the least of these. Then n is a natural prime. For otherwise, n could be factored into a product $n'n''$ of smaller natural numbers and, by the unique factorization property, either n' or n'' would be divisible by π, contradicting the assumption that n is the least natural number divisible by π. Hence, n is a natural prime p divisible by π. To prove the uniqueness of p, assume that q is another natural prime divisible by π. Then there exist rational integers x, y such that $px + qy = 1$, from which it follows that π is a divisor of 1, which is obviously false. Hence, the natural prime such that π divide p is unique. Then (3) follows from this and (2).*
4. *Let p be an odd natural prime not divisor of d and such that d is a quadratic residue modulo p. Then there exist a natural number n such that p is divisor of $n^2 - d = (n - \sqrt{d})(n + \sqrt{d})$. If p were a prime of $\mathbb{Z}[\sqrt{d}]$, then one of the factors $n - \sqrt{d}$ and $n + \sqrt{d}$ would be divisible by p. But, then, $N(p) = p^2 | N(n - \sqrt{d}) = n^2 - d$ and $p | n + \sqrt{d} = \frac{n^2-d}{n-\sqrt{d}}$ so that $p|2n$ and p being odd $p|n$ and then $p|d$ which is in contradiction with the assumptions. Therefore, p is not prime in $\mathbb{Z}[\sqrt{d}]$ but the product of 2 prime by (2).*

Conversely, let p be an odd natural prime not divisor of d and equal to the product of $\pi'\pi''$ of prime of $\mathbb{Z}[\sqrt{d}]$. Then we can write $\pi' = a+b\sqrt{d}$ and $N(\pi') = a^2-db^2 = p$, so that $a^2 \equiv db^2$ mod p. Now, b cannot be divisible by p, because this would imply that a, hence also π' would be divisible by p, which is obviously false. So, there is a rational integer w such that $wb \equiv 1$ mod p. Hence, $d \equiv w^2a^2$ mod p, i.e. d is quadratic residue modulo p.

Now we go back to the present exercise with $d = 2$, and remember that by Gauss lemma, 2 is a quadratic residue mod 8 if and only if $p \equiv \pm 1$ mod 8. As a consequence we have that the prime of $\mathbb{Z}$ which are also prime on $\mathbb{Z}[\sqrt{2}]$ are the prime congruent to ± 3 modulo 8, the element of $\mathbb{Z}[\sqrt{2}]$ whose norm is a natural prime congruent to ± 1 modulo 8; the number whose norm equals 2, i.e the number $\sqrt{2}$ an associates.

If you have forgotten:

1. Let p be an odd prime and $a \in \mathbb{Z}$ not divisible by p. Then a is called a **quadratic residue mod** p if $x^2 \equiv a \ mod \ p$ has a solution and a **quadratic non residue modulo** p if $x^2 \equiv a \ mod \ p$ has no solution.

2. Let p be an odd prime. The **Legendre symbol** is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is quadratic residue mod } p \\ -1 & \text{if } a \text{ is quadratic non residue mod } p \\ 0 & \text{if } p|a. \end{cases}$$

Euler's Criterion Let p be an odd prime and a an integer not divisible by p.

1. There are exactly $(p-1)/2$ quadratic residues mod p and $(p-1)/2$ quadratic non-residue mod p

2. $x^2 \equiv a \mod p$ has a solution if and only if

$$a^{(p-1)/2} \equiv 1 \mod p.$$

   More precisely,

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \ mod \ p$$

Proof of Euler Criterion:

1. *Consider the residue classes 1^2, 2^2, ..., $((p-1)/2)^2$ mod p. Since $a^2 \equiv (-a)^2$ mod p, these are all quadratic residues modulo p. They are also distinct, from $a^2 \equiv b^2$ mod p would follow $a \equiv \pm b$ mod p and when $1 \leq a, b \leq (p-1)/2$ this implies $a = b$. So there are exactly $(p-1)/2$quadratic residues modulo p. The remaining $p-1-(p-1)/2 = (p-1)/2$ residue classes are of course quadratic non residues.*

2. *Clear, if $a \equiv 0$ mod p. So assume, $a \not\equiv 0$ mod p. Since $(a^{(p-1)/2})^2 \equiv a^{p-1} \equiv 1$ mod p by Fermat's little theorem we see that $a^{(p-1)/2} \equiv \pm 1$ mod p. Suppose that a is a quadratic residue, i.e there is an integer x such that $x^2 \equiv a$ mod p. Then $1 = x^{p-1} \equiv (x^2)^{(p-1)/2} \equiv a^{(p-1)/2}$ mod p, which proves half of our assertion. Since we work in the field $\mathbb{Z}/p\mathbb{Z}$, the equation $x^{(p-1)/2} \equiv 1$ mod p has at most $(p-1)/2$ solutions. We know these solutions to be the $(p-1)/2$ quadratic residues. Hence, $a^{(p-1)/2} \equiv -1$ mod p, for any quadratic non residue a mod p.*

We can be reformulated Euler Criterion in more group-theoretic language as follows. The map

$$(\mathbb{Z}/p\mathbb{Z})^* \simeq \{\pm 1\}$$

that sends a to $a^{(p-1)/2} \pmod p$ is a homomorphism of groups, whose kernel is the subgroup of squares of elements of $(\mathbb{Z}/p\mathbb{Z})^*$.

Corollary: Let p be an odd prime and a, $b \in \mathbb{Z}$. Then,

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

<u>*Proof of Corollary:*</u>

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{(p-1)/2}b^{(p-1)/2} \equiv (ab)^{(p-1)/2} \equiv \left(\frac{ab}{p}\right) \ mod\ p$$

Because Legendre symbols can only be 0, ± 1 *and* $p \geq 3$, *the strict equality* $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ *follows.*

Corollary: Let p be an odd prime. Then, $\left(\frac{1}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = \begin{cases} 1 & if\ p \equiv 1\ mod\ 4 \\ -1 & if\ p \equiv -1\ mod\ 4 \end{cases}$

<u>*Proof of Corollary:*</u> *Of course,* $\left(\frac{1}{p}\right) = 1$ *is trivial. Also, we know that* $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2}\ mod\ p$. *Since* $p \geq 3$ *strict equality follows.*

We say that the residue classes 1, 2, ..., $(p-1)/2$ mod p are called **positive**, the residue classes -1, -2, ..., $-(p-1)/2$ mod p are called **negative**. **Gauss Lemma** Let p be an odd prime and let a be an integer $\not\equiv 0 \pmod{p}$. Form the numbers

$$a,\ 2a,\ 3a,\ \ldots,\ \frac{p-1}{2}a$$

and reduce them modulo p to lie in the interval $(-\frac{p}{2},\ \frac{p}{2})$. Let μ be the number of negative residue classes mod p. Then

$$(\frac{a}{p}) = (-1)^{\mu}.$$

<u>*Proof of Gauss lemma:*</u> *In defining* ν, *we expressed each number in*

$$S = \left\{a, 2a, \ldots, \frac{p-1}{2}a\right\}$$

as congruent to a number in the set

$$\left\{1, -1, 2, -2, \ldots, \frac{p-1}{2}, -\frac{p-1}{2}\right\}.$$

No number $1, 2, \ldots \frac{p-1}{2}$ *appears more than once, with either choice of sign, because if it did then either two elements of* S *are congruent modulo* p *or* 0 *is the sum of two elements of* S, *and both events are impossible. Thus the resulting set must be of the form*

$$T = \left\{\epsilon_1 \cdot 1, \epsilon_2 \cdot 2, \ldots, \epsilon_{(p-1)/2} \cdot \frac{p-1}{2}\right\},$$

where each ϵ_i is either $+1$ or -1. Multiplying together the elements of S and of T, we see that

$$(1a)\cdot(2a)\cdot(3a)\cdot\dots\cdot\left(\frac{p-1}{2}a\right)\equiv(\epsilon_1\cdot 1)\cdot(\epsilon_2\cdot 2)\cdots\left(\epsilon_{(p-1)/2}\cdot\frac{p-1}{2}\right)\pmod p,$$

so

$$a^{(p-1)/2}\equiv\epsilon_1\cdot\epsilon_2\cdot\dots\cdot\epsilon_{(p-1)/2}\pmod p.$$

The lemma then follows from Euler Criterion.

When 2 is a quadratic residue: Let p be an odd prime. Then, $\left(\frac{2}{p}\right)=\begin{cases}1 & if\ p\equiv\pm1\ mod\ 8\\ -1 & if\ p\equiv\pm3\ mod\ 8\end{cases}$

Proof: *We apply Gauss' lemma. To do so we must count μ, the number of negative residue among 2, 4, ..., $p-1$ mod p. So,*

$$\mu=\sharp\{n\ even|(p+1)/2\le n\le p-1\}=\sharp\{n|(p+1)/4\le n\le(p-1)/2\}$$

Replace n by $(p+1)/2-n$ to obtain

$$\mu=\sharp\{n|1\le n\le(p+1)/4\}=[(p+1)/4]$$

This implies that μ is even if $p\equiv\pm1$ mod 8 and μ is odd if $p\equiv\pm3$ mod 8. Gauss lemma now yields our assertion.

Notice that

$$(\frac{2}{p})=(-1)^{(p^2-1)/8}$$

Exercise 1 p 15 [N]:
Is $\frac{3+2\sqrt{6}}{1-\sqrt{6}}$ an algebraic integer ?

Solution:

$$\frac{3+2\sqrt{6}}{1-\sqrt{6}} = \frac{(3+2\sqrt{6})(1+\sqrt{6})}{-5} = \frac{15+5\sqrt{6}}{-5} = -3-\sqrt{6}$$

Now, $\frac{3+2\sqrt{6}}{1-\sqrt{6}} = -3-\sqrt{6}$ *is a root of the polynomial:*

$$(x+3+\sqrt{6})(x+3-\sqrt{6}) = x^2+6x+3$$

which has integral coefficient so that $\frac{3+2\sqrt{6}}{1-\sqrt{6}}$ *is an algebraic integer.*

Exercise 2 p 15 [N]:
Show that, if the integral domain A is integrally closed, then so is the polynomial ring $A[t]$.

Solution:
Let $K = \{a/b | a, b \in A, b \neq 0\}$ *be the fraction field of* A*. Then* A *is integrally closed means that* A *is integrally closed in* K*, i.e. if* $\alpha \in K$ *is integral over* A *then we must have* $\alpha \in A$*. Now,* $k(t)$ *is the fraction field of* $A[t]$ *then we must have* $\alpha(t) \in A[t]$*.*

Claim: *If* $f(t)$*,* $g(t) \in K[t]$ *are monic polynomials such that* $f(t) \cdot g(t) \in A[t]$ *then* $f(t)$*,* $g(t) \in A[t]$*.*
Proof of the claim: *Write* $f(t) = \prod_{i=1}^{l}(x-a_i)$ *and* $g(t) = \prod_{j=1}^{m}(x-b_i)$*. The roots* a_i*,* b_j *must be integral over* A *since* $f(t)g(t)$ *is a monic polynomial with coefficients in* R*. On the other hand, the coefficients of* f*,* g *lie in* K*. But* A *is integrally closed by assumption which implies that the coefficients of* f*,* g *must lie in* A*.*

We now conclude the proof that $A[t]$ *is integrally closed* $K(t)$*. Assume that* $f(t) \in K(t)$ *is monic (we may need to add a high power of* t *to* $f(t)$ *to arrange this and integral over* $A[t]$*, i.e., satisfies a polynomial equation*

$$f(t)^n + a_{n-1}f(t)^{n-1} + ... + a_1 f(t) + a_0 = 0, \quad (a_i \in A[t])$$

Then we must have

$$f(t) \cdot (f(t)^{n-1} + a_{n-1}f(t)^{n-2} + \cdots + a_1) = -a_0 \in A[t]$$

The lemma immediately gives that $f(t) \in A[t]$*.*