Quadratic Residues Part 1.

Let p be prime

<u>Defn</u> x is a <u>quadratic residue mod p</u> if $x = y^2 \bmod p$ for some $y \in \mathbb{Z}_p^* = G_p$

<u>Lemma</u> The quadratic residues form a group of index 2 in $\mathbb{Z}_p^* = G_p$

<u>Proof</u> $1^2 = 1$. If $x_1 = y_1^2$ and $x_2 = y_2^2$ for $y_1, y_2 \in \mathbb{Z}_p^*$

then $x_1 x_2 = (y_1 y_2)^2$ and $x_1^{-1} = (y_1^{-1})^2$

Let Q be the group of quadratic residues.

Of <u>index 2</u> means that $|Q| = \frac{1}{2}(p-1) = \frac{1}{2}|\mathbb{Z}_p^*|$

Since $\mathbb{Z}_p^*$ contains a primitive element we have $\mathbb{Z}_p^* = \{a^k, 1 \le k \le p-1\}$

Clearly $Q \supset \{a^{2k} : 1 \le k \le \frac{p-1}{2}\}$. If $a^m \in Q$ for some odd m

then $a \in Q$ and $a = b^2$, since b. But then $b^{p-1} \equiv 1 \bmod p$

$\Rightarrow a^{\frac{p-1}{2}} \equiv 1 \bmod p$ X. So $|Q| = \frac{1}{2}(p-1)$ $\square$

<u>Theorem</u> Let p be any odd prime. Then -1 is a quadratic residue mod $p \iff p \equiv 1 \bmod 4$

<u>Proof</u> If $-1 = y^2$ then $y^4 \equiv 1 \bmod p \Rightarrow 4 \mid p-1 \Rightarrow p \equiv 1 \bmod 4$

Conversely let $p \equiv 1 \bmod 4$ and let a be a primitive element.

$p - 1 = 4k \Rightarrow a^{4k} \equiv 1 \bmod p \Rightarrow (a^{2k})^2 \equiv 1 \bmod p$

$\Rightarrow (a^{2k}-1)(a^{2k}+1) \equiv 0 \bmod p \Rightarrow a^{2k} \equiv -1$

$\Rightarrow -1 = (a^k)^2$ $\square$

<u>Examples</u> $5 \equiv 1 \bmod 4$. $4 \equiv -1 \bmod 5$. $4 = 2^2$ is a quadratic residue mod 5

$7 \equiv 3 \bmod 4$. The quadratic residues mod 7 are $1 = (\pm 1)^2$, $4 \equiv (\pm 2)^2$ and $2 \equiv (\pm 3)^2$. $-1 \equiv 6$ is not a quadratic residue mod 7.

Applicatn

<u>Theorem</u> $n \in \mathbb{Z}_+$ is a sum of 2 integer squares

$\iff n = N^2 2^k \prod_{i=1}^{r} p_i$ where p_i is odd prime and

$p_i \equiv 1 \bmod 4$, $N \in \mathbb{Z}$ and $k \in \mathbb{N}$

Proof Later (We need to review some ring theory first.

<u>Check of plausibility</u> $1 = 0^2 + 1$

$5 = 2^2 + 1$

$10 = 3^2 + 1$

$20 = 4^2 + 2^2$

$25 = 5^2 + 0^2 = 3^2 + 4^2$

$26 = 2 \times 13 = 5^2 + 1^2$

$6 = 2 \times 3$ is not a sum of 2 squares

$21 = 3 \times 7$ — ~~does~~ not a sum of 2 squares $21 \equiv 1 \bmod 4$

but $3 \equiv 3 \bmod 4$, $7 \equiv 3 \bmod 4$.

More on the theorem later, Just a few preliminary results:

<u>Lemma</u> If $a^2 + b^2$ is odd and $a, b \in \mathbb{Z}_+$ then $a^2 + b^2 \equiv 1 \bmod 4$

<u>Proof</u> W.l.g. a is odd and b is even. Then $a^2 \equiv 1 \bmod 4$

(in fact $a^2 \equiv 1 \bmod 8$) and $b^2 \equiv 0 \bmod 4$

So $a^2 + b^2 \equiv 1 \bmod 4$ □.

<u>Lemma</u> If each of n_1 and n_2 is a sum of 2 integer squares, then so is $n_1 n_2$.

Proof $n_1 = a_1^2 + b_1^2 = |a_1 + ib_1|^2$ $n_2 = a_2^2 + b_2^2 = |a_2 + ib_2|^2$

Then $n_1 n_2 = |(a_1 + ib_1)(a_2 + ib_2)|^2 = |(a_1 a_2 - b_1 b_2) + i(a_1 b_2 + a_2 b_1)|^2$

$= (a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + a_2 b_1)^2$ □

<u>Lemma</u> If p is prime and $p \equiv 1 \bmod 4$ then $\exists\, n \in \mathbb{Z}_+$ and $k \in \mathbb{Z}_+$ s.t. $np = 1 + k^2$

<u>Proof</u> -1 is a quadratic residue mod p. So $\exists\, k \in \mathbb{Z}_+$ s.t. $k^2 \equiv -1 \bmod p$. That is, $k^2 + 1 = np$ for some $n \in \mathbb{Z}_+$ □

Groups, Rings and Fields

A group G is a set G with a binary operation $\times$ often called multiplication which satisfies the usual rules we associate with multiplication
$\forall x, y \in G \quad xy \in G$ exists and the following rules hold.

Associative $(xy)z = x(yz) \quad \forall x, y, z \in G.$
Identity $\exists\ 1 \in G$ s.t. $1x = x1 = x \quad \forall x \in G.$
Inverses $\forall x \in G \ \exists\ x^{-1} \in G$ s.t. $xx^{-1} = x^{-1}x = 1 \in G.$

If an identity exists it follows that it is unique
Similarly the axioms force us that ~~the~~ inverses are unique

The examples we are interested in are mainly finite and (or abelian) commutative. Multiplication is commutative if
$xy = yx \quad \forall x, y \in G.$

Main example so far of a commutative finite group has been G_n - group of units in $\mathbb{Z}_n$, in particular $G_p = \mathbb{Z}_p^*$ if p is prime. We have already used the classification of finite commutative groups to describe G_n, as Any finite abelian group is a product of cyclic groups.

For abelian groups the multiplication is often written as $+$, the identity as 0 and the inverse of x as $-x$

(5/46)

For example $\mathbb{Z}_n$ is an abelian group under addition with "identity" 0 $\quad x+0=0+x=x \quad \forall x\in\mathbb{Z}_n$

$$x+(-x)=(-x)+x=0 \quad \forall x\in\mathbb{Z}_n.$$

$\mathbb{Z}_n$ is not a group under multiplication (unless $n=0$) because 0 does not have an inverse in $\mathbb{Z}_n$ if $n>0$ — because $1\neq 0$ is the identity.

However $\mathbb{Z}_n^*$ is a group under mult^n $\Leftrightarrow$ n is prime.

<u>Rings</u>

A ring R is a set with $\underline{2}$ binary operations $+$ and $\cdot$ such that $(R,+)$ is an abelian group with "identity element 0 and $-x$ denotes the additive inverse of x

- $\cdot$ is associative $(x\cdot y)\cdot z = x\cdot(y\cdot z)$ $\forall x,y,z\in R$.
- $\cdot$ is distributive over $+$
  $x\cdot(y+z) = (x\cdot y)+(x\cdot z)$ $\forall x,y,z\in R$
  $(y+z)\cdot x = (y\cdot x)+(z\cdot x)$

It follows from the axioms that $0.x = x.0 = 0$ $\forall x\in R$

A ring R is commutative if the multiplication is commutative.

and is a ring with identity if $\exists$ an identity element for multip^n (usually called 1)

$$1.x = x.1 = x \quad \forall x\in R.$$

~~It follows from the axioms that $0.x = x.0 = 0$ $\forall x\in R$~~

Example $\mathbb{Z}$ is a commutative ring with 1. So is $\mathbb{Z}_n$ $(n\geq 2)$

So are $\mathbb{R}$, $\mathbb{C}$

So is $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$, the ring of Gaussian integers

If R is a commutative ring then

$R[x] = \{a_0 + a_1 x + \dots + a_n x^n : n \in \mathbb{N}, a_i \in R\}$

is another commutative ring, the ring of polynomials with coefficients in R e.g. $(x+1)(x+1) = x^2+1$ in $\mathbb{Z}_2[x]$.

We shall be particularly interested in $\mathbb{Z}[x]$ and in $\mathbb{Z}_n[x]$ – especially when n is prime. In fact we have already made use of this.

Defn A commutative ring with identity is an integral domain if it has no zero divisors, that is, $xy=0 \Rightarrow x=0$ or $y=0$

Examples $\mathbb{Z}$ is an integral domain.

$\mathbb{Z}_n$ is an integral domain $\Leftrightarrow$ n is prime

e.g. $\mathbb{Z}_2$ is an integral domain but $\mathbb{Z}_4$ is not: $2\times2 \equiv 0 \bmod 4$

$R[x]$ is an integral domain $\Leftrightarrow$ R is an integral domain

e.g. $\mathbb{Z}_2[x]$ is an integral domain but $\mathbb{Z}_4[x]$ is not.

Defn For $a, b \in R$ a divides b (in R), written $a \mid b$, iff

$b = ac$ for some $c \in R$

A unit (in R) is a divisor of 1.

Prime and irreducibles

Let R be an integral domain

$p \in R$ is irreducible if $p \neq 0$, p is not a unit, and

$p = ab \Rightarrow a$ or b is a unit.

$p \in R$ is prime if $p \neq 0$, p is not a unit and

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b.$$

Lemma
In any integral domain, p prime $\Rightarrow$ p irreducible

Proof
Suppose p is prime and $p = ab$. w.l.g. $p \mid b$

So $cp = b$ for some $c \in R$.

So $p = acp$. $(1-ac)p = 0$

No zero divisors, $p \neq 0 \Rightarrow 1-ac = 0 \Rightarrow a$ is a unit $\square$

In many of the rings we are interested in, primes and irreducibles are the same.

True in $\mathbb{Z}$. True in $\mathbb{Z}_p[x]$, p prime.

This is because these rings are examples of Euclidean domains

Let R be any commutative ring.

Defn A function $V: R \setminus \{0\} \to \mathbb{N}$ is a Euclidean valuation (or Euclidean function) if

1. $V(a) \leq V(ab)$ $\forall a, b \neq 0$
2. $a, b \neq 0 \Rightarrow b = qa + r$ with $r = 0$ or $V(r) < V(a)$.

Defn An integral domain with a Euclidean valuation is called a Euclidean domain

<u>Examples</u> $\mathbb{Z}$ is a Euclidean domain with valuation

$V(n) = |n|_{\mathbb{Z}\setminus\{0\}}$

$\forall a, b \in \mathbb{Z}$ $\exists q, r \in \mathbb{Z}$ with

$b = qa + r \qquad |r| < |a|$

$\mathbb{Z}[x]$ has no Euclidean valuation but $\mathbb{Q}[x]$ is a Euclidean domain with valuation $\deg(f(x)) = V(f)$

Similarly $\mathbb{Z}_p[x]$ is a Euclidean domain with valuation

$V(f) = \deg(f)$

$\mathbb{Z}[i]$ is a Euclidean domain with valuation

$V(a_1 + a_2 i) = |a_1 + a_2 i|^2 = a_1^2 + a_2^2 \qquad (a_1, a_2 \in \mathbb{Z})$

To see this, given $b, a \in \mathbb{Z}[i]$ with $a \neq 0$ consider

$\frac{b}{a} = x_1 + x_2 i \qquad x_1, x_2 \in \mathbb{R}$ (in fact $x_1, x_2 \in \mathbb{Q}$)

Then $\exists$ $q_1, q_2 \in \mathbb{Z}$ with $|q_1 - x_1| \leq 1/2 \quad |q_2 - x_2| \leq 1/2$

Put $q = q_1 + q_2 i \qquad r = b - qa \in \mathbb{Z}[i]$

$\left| b/a - q \right| = \sqrt{(q_1 - x_1)^2 + (q_2 - x_2)^2} \leq \sqrt{1/2} \qquad \left|\frac{b}{a} - q\right|^2 \leq 1/2$

$|r|^2 = \left| a\left(\frac{b}{a} - q\right)\right|^2 \leq 1/2 |a|^2 \qquad V(r) < V(a)$ as reqd.

Defn A <u>field</u> is an integral domain ~~that~~ such that every element of $F\setminus\{0\}$ is a unit.

This means that ~~every element~~ $F\setminus\{0\}$ is a commutative group under multiplication.

$\mathbb{Z}_n$ is a field $\Leftrightarrow$ n is prime.

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

In general $F[x]$ is a Euclidean domain with valuation $V(f) = \deg(f)$.

For Euclidean domains, many of the results proved for $\mathbb{Z}$ can be proved in exactly the same way.

For example, if R is a Euclidean domain:

Thm The g.c.d. of any $m, n \in R \setminus \{0\}$ is any element of the form $am + bn \neq 0$ s.t. $V(am+bn)$ is minimal.

The g.c.d. is unique up to multiplication by a unit.

__Example__ 2 or -2 is the g.c.d. of 6 and -4 in $\mathbb{Z}$.

__Thm__ If R is a Euclidean domain and $m, p \in R \setminus \{0\}$ with $\gcd(m,p) = 1$ and $p \mid mn$, then $p \mid n$.

It follows that if R is a Euclidean domain then R is a __unique factorisation domain__ (UFD) - a fact which has already been used for $\mathbb{Z}_p[x]$.

__Def__^{n} An integral domain R is a __UFD__ if whenever $x \in R$, $x \neq 0$, x not a unit, then $x = v \prod_{i=1}^{r} p_i^{k_i}$ where p_i is prime, v is a unit, $p_i \neq u p_j$ for any $i \neq j$ and unit u, $k_i \in \mathbb{Z}_+$, and this representation is essentially unique that is, if $x = v' \prod_{i=1}^{s} q_i^{l_i}$ is a similar representation then $r = s$ and after renumbering, $k_i = l_i$ for $1 \leq i \leq s$ and $q_i = u_i p_i$ for some unit u_i.

Examples

$\mathbb{Z}[i]$ is a unique factorisation domain

e.g. ~~$2 = i(1+i)^2$ is the prime decomposition~~ of 2

~~Can~~ $2 = -i(1+i)^2$ is the prime decomposition of 2

Can also write $2 = i(1-i)^2$ Note that $i(1-i) = 1+i$

$1+i$ is prime in $\mathbb{Z}[i]$ (and so is $1-i$) because $V(1+i) = 2$ is prime in $\mathbb{Z}$ and, in $\mathbb{Z}[i]$, $V(a) = 1 \iff a$ is a unit $\iff a = \pm 1$ or $\pm i$

$\mathbb{Z}_p[x]$ is a unique factorisation domain

$$x^{p-1} - 1 = \prod_{n \in \mathbb{Z}_p^*} (x - n) \qquad x - n \text{ is prime in } \mathbb{Z}_p[x]$$

Other examples of Euclidean domains

Let D be any integer that is not a perfect square

e.g. $D = \pm 2, \pm 3, -1, -4, \pm 5, \pm 6, \pm 7$

Then $\sqrt{D}$ is not rational. In fact if $D < 0$ then $\sqrt{D}$ is not real (and is purely imaginary).

$\mathbb{Z}[\sqrt{D}]$ is a ring. $\mathbb{Q}[\sqrt{D}]$ is a field.

We can define $V : \mathbb{Z}[\sqrt{D}] \longrightarrow \mathbb{N}$ by

$$V(c_1 + c_2\sqrt{D}) = |c_1^2 - c_2^2 D| \quad \text{for } c_1, c_2 \in \mathbb{Z}.$$

$V(c) = 0 \iff 0 \iff c = 0$

$V(cd) = V(c)V(d)$ So $V(c) \leq V(cd)$ $\forall c, d \in \mathbb{Z}[\sqrt{D}] \setminus \{0\}$

This is the first condition of a Euclidean valuation

What about the second condition? Sometimes yes, sometimes no.

Def^n If $D \equiv 1 \bmod 4$ $(D = -3, 5, 13, \ldots)$ not an integer square

then we can define

$$\mathcal{O}(\sqrt{D}) = \{c_1 + c_2\sqrt{D} : c_1 + c_2 \in \mathbb{Z} \wedge c_1 - c_2 \in \mathbb{Z}\} = \mathbb{Z}\left[\tfrac{1+\sqrt{D}}{2}\right]$$

This, too, is a ring and

$$v(c_1 + c_2\sqrt{D}) = |c_1^2 - c_2^2 D| \in \mathbb{N}$$

satisfies the same conditions as before

(Alaca Props 2.2. – 2.9?)

Theorem v is a Euclidean valuation on $\mathbb{Z}[\sqrt{D}]$

$\Leftrightarrow$ $D = -1, \pm 2, 3, 6, 7, 11, 19$ or 57

v is a Euclidean valuation on $\mathcal{O}[\sqrt{D}]$ $\Leftrightarrow$

$D = -3, -7, -11, 5, 13, 17, 21, 29, 33, 37, 41, 73$

The ring $\mathbb{Z}[x]$

$\mathbb{Z}[x]$ is an example of a ring which is not a Euclidean domain for any Euclidean valuation, but is is a UFD. To see that degree is not a Euclidean valuation, we cannot write

$$x^2 = q(x)(2x+1) + r(x) \quad \text{with } r(x) \in \mathbb{Z} \text{ and}$$

$$q(x) \in \mathbb{Z}[x].$$

Because $\mathbb{Z}[x]$ is a UFD, any polynomial in $\mathbb{Z}[x]$ can be written essentially uniquely as a product of irreducibles in $\mathbb{Z}[x]$. The only units in $\mathbb{Z}[x]$ are ± 1

Particularly interesting cases are the polynomials

$x^n - 1 \qquad n \in \mathbb{Z}_+$

$$\text{e.g.} \quad x^2 - 1 = (x-1)(x+1)$$
$$x^3 - 1 = (x-1)(x^2+x+1)$$
$$x^4 - 1 = (x-1)(x+1)(x^2+1)$$

$x^d - 1 \mid x^n - 1$ in $\mathbb{Z}[x] \Leftrightarrow d \mid n$. If $n = dk$ then

$$x^n - 1 = (x^d - 1)\left(\sum_{i=0}^{k-1} x^{id}\right)$$

~~The~~ To write $x^n - 1$ as a product of irreducibles we use the cyclotomic polynomials $\Psi_d(x)$ for d dividing n. We can define

$$\Psi_d(x) = \gcd_{\mathbb{Z}[x]}\left(\cancel{\ }, \sum_{k=0}^{d/d_1 - 1} x^{kd_1} : 1 \le d_1 < d,\ d_1 \mid d \right)$$

or alternatively

$$\Psi_d(x) = \mathrm{lcm}\left(\frac{x^d - 1}{x^{d_1} - 1} : 1 \le d_1 < d,\ d_1 \mid d \right)$$

~~This is also Ψ?~~

We also have $\Psi_d(x) = \prod_{\substack{1 \le r < d \\ \gcd(r,d)=1}} \left(x - e^{\frac{2\pi i r}{d}}\right)$

or $\Psi_d(x)$ can be defined inductively by

$$x^d - 1 = \prod_{\substack{d_1 \mid d \\ 1 \le d_1 \le d}} \Psi_{d_1}(x)$$

The first 2 definitions make it clear that $\Psi_d(x)$ has integer coefficients, that is, that $\Psi_d(x) \in \mathbb{Z}[x]$ — once we know that $\mathbb{Z}[x]$ is a UFD. The first 2 definitions are clearly equivalent, since if $d = kd_1$ then $x^d - 1 = (x^{d_1} - 1)\sum_{i=0}^{k-1} x^{i d_1}$. The last two properties then follow by induction.

The polynomials $\Psi_d(x)$ might not be irreducible in $\mathbb{Z}_p[x]$ for different primes p e.g.

$$\Psi_3(x) = x^2 + x + 1 = (x-1)^2 \text{ in } \mathbb{Z}_3[x]$$

$$\Psi_4(x) = x^2 + 1 = (x-2)(x-3) \text{ in } \mathbb{Z}_5(x)$$