Math 312, lecture 21, 13/6/2018

Last time: the Jacobi Symbol

Today: ① Safe primes

② The Gaussian integers

Q: How to test if $a \bmod m$ is a primitive root?

A: if $a^d \not\equiv 1 \ (m)$ then the order of a is not any divisor of d

(see PS)

Q: What is the order of a^k (mod m)? A: PS: $\dfrac{\mathrm{ord}_m(a)}{(k, \mathrm{ord}_m(a))}$.

Recall: A prime q is safe if $q = 2p+1$ where p (odd) is prime (then p is called a Sophie Germain prime)

Fix a safe prime q (11, 23, ...).

Consider a class $a \bmod q$ $(a \not\equiv 0 \ (q))$

$$\mathrm{ord}_q(a) \mid q-1 = 2p \qquad \text{so} \quad \mathrm{ord}_q(a) \in \{1, 2, p, 2p\}$$

↑ Fermat's little thm

Also, $\mathrm{ord}_q(a) = 1$ iff $a \equiv 1 \ (q)$, $\mathrm{ord}_q(a) = 2 \iff a \equiv -1 \ (q)$

$x^2 \equiv 1 \ (q)$ $\Downarrow$ $x \equiv \pm 1 \ (q)$ + $(-1)^2 \equiv 1 \ (q)$ but $-1 \not\equiv 1 \ (q)$

Conclusion: let q be a safe prime, $a \not\equiv \pm 1, 0$ (q)

Then $\mathrm{ord}_q(a) = \begin{cases} p & \left(\frac{a}{q}\right) = 1 \\ 2p & \left(\frac{a}{q}\right) = -1 \end{cases}$

Application: Diffie-Hellman Key exchange

Problem: Alice & Bob ~~would~~ need to have a shared secret.

Solution: Alice & Bob agree publicly to a large prime q and a class a mod q. (need a to have large order mod q)

Alice (secretely) chooses exponent k

Bob (secretely) " " l.

Alice sends a^k to Bob

Bob sends a^l to Alice

(at the moment Alice knows (k, a^l)

Bob knows (l, a^k))

Alice computes $a^{kl} \equiv (a^l)^k$ (q)

Bob computes $a^{kl} \equiv (a^k)^l$ (q)

$\Big\}$ a^{kl} is the shared secret.

(try with your study partner!)

Review I: the Gaussian Integers (not examinable material)

Def: $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$, i formal number st: $i^2=-1$

E.g.: $2+i$, $3-5i$, i, 1, 2, 0, ...

$2+i = 2+1\cdot i$, $i = 0+1\cdot i$, $2 = 2+0i$, $0 = 0+0i$

Def: $(a+bi)+(c+di) = (a+c)+(b+d)i$ $\qquad (2+i)+(3-5i) = 5-4i$

$$(a+bi)(c+di) = ac + bc\cdot i + ad\cdot i + b\cdot d\cdot i\cdot i \leftarrow i^2=-1$$
$$= (ac-bd)+(ad+bc)i$$

$$(2+i)(3-5i) = 2\cdot 3 - 10i + 3i - 5i^2 = 6+5-7i = 11-7i$$

Fact: Usual laws of arithmetic hold:
$$(x+y)+z = x+(y+z)$$
$$x+y = y+x$$
$$0+x = x$$
$$(a+bi)+((-a)+(-b)i) = 0$$
$$\vdots$$

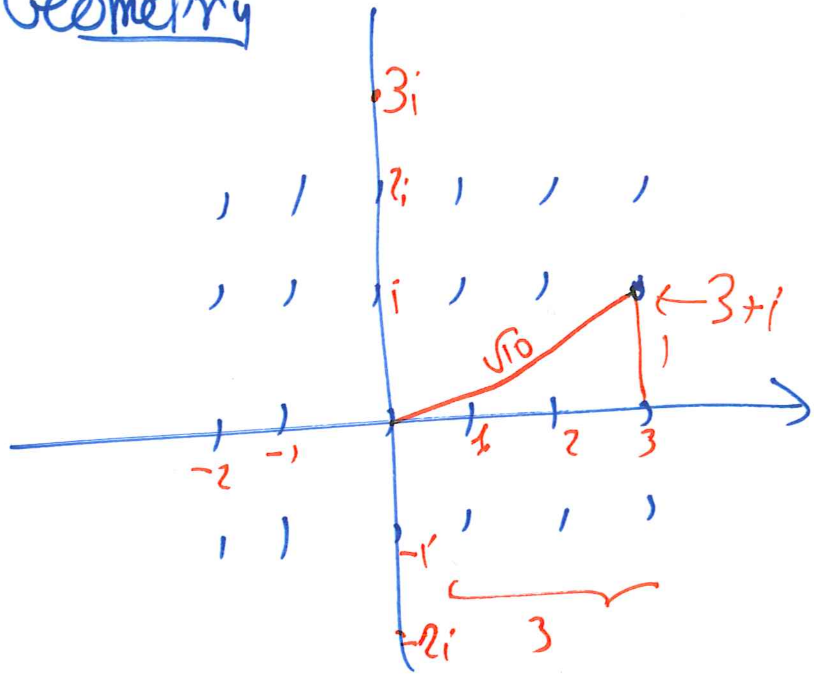
Observation: If $z = a+bi$ set $\bar{z} = a-bi$

$$\overline{2+i} = 2-i, \quad \overline{3-5i} = 3+5i$$

then: $\overline{z+w} = \bar{z}+\bar{w}$, $\overline{z\cdot w} = \bar{z}\cdot\bar{w}$.

Def: $Nz \overset{\text{def}}{=} z\cdot\bar{z}$ if $z = a+bi$, $N(z) = a^2+b^2$

Geometry



$N(3+i) = 3^2 + 1^2 = 10$

"Well-ordering": Every non-empty set of Gaussian integers has an element of smallest norm ($\Leftrightarrow$ smallest magnitude)

Pf: Let A be a set of Gaussian integers. Then set $B = \{ Nz : z \in A \}$ is a set of non-negative rational integers, so has a least member.

Observe: $N(zw) = (zw)(\overline{zw}) = z \cdot w \cdot \bar{z} \cdot \bar{w} = z \cdot \bar{z} \cdot w \cdot \bar{w}$
$= (Nz)(Nw)$

Def: Let $z, w \in \mathbb{Z}[i]$. Say z divides w, write z / w if $\exists x \in \mathbb{Z}[i]$ s.t. $w = z \cdot x$

E.g. $10 = 3^2 + 1^2 = (3+i)(3-i)$ so $3+i / 10$, $3-i / 10$

Also, $\frac{3+i}{1+i} = \frac{3+i}{1+i} \cdot \frac{1-i}{1-i} = \frac{3\cdot 1 - i^2 + i - 3i}{1^2+1^2} = \frac{4-2i}{2} = 2-i$

so $1+i \mid 3+i \mid 10$, so $1+i \mid 10$ also

~~Note~~ Observe: If $z \mid 1$ then $Nz \mid N1$ so $Nz \in \{\pm 1\}$

$\uparrow$ divisibility in $\mathbb{Z}$

(but $Nz \geq 0$) so $Nz = 1$

Conversely, if $Nz = 1$ then $z \cdot \bar{z} = 1$ so $z \mid 1$

Bottom line: In $\mathbb{Z}$, x divides all integers iff $x = \pm 1$

In $\mathbb{Z}[i]$, x " everything iff $x \in \{\pm 1, \pm i\}$

(if $x = a+bi$, $a^2+b^2=1$ forces $a^2=1, b=0$ or $b^2=1, a=0$)

Def: Call $z \in \mathbb{Z}[i]$ irreducible if $Nz \neq 0, 1$ and in every factorization $z = xy$ either x or y has norm 1

(i.e. only factorizations are:

$z = 1 \cdot z$, $z = (-1)\cdot(-z)$

$z = i(-iz)$, $z = (-i)\cdot(iz)$)

Thm: Every $z \in \mathbb{Z}[i]$ other than 0 is pdt of irreducibles (and possibly a unit $\varepsilon \in \{1, -1, i, -i\}$.)

Eg: $10 = (3+i)(3-i) = (1+i)(2-i)(1-i)(2+i)$

$N(1\pm i) = 1^2+1^2 = 2$, $N(2 \pm i) = 2^2+1^2 = 5$

2,5 prime in $\mathbb{Z}$, so $N(1\pm i)$, $N(2\pm i)$ can't be factored,

so $1\pm i$, $2\pm i$ can't be factored unless a factor has norm 1.

Pf of thm: let a $z \in \mathbb{Z}[i]$ have smallest magnitude among all non-zero numbers not of the form $\varepsilon \cdot \prod_{j=1}^{r} p_j$ where $\varepsilon \in \{\pm 1, \pm i\}$, p_j irreducible

Then $|z| > 1$ (if $|z| = 1$, z is a unit).

If z were irreducible, we'd be done

else, $z = xy$, $Nx, Ny \neq 1$ so $Nx, Ny < Nz$.

(since $Nx \cdot Ny = Nz$)

so x, y are pdts of irreducibles, hence so is z. $\Rightarrow\Leftarrow$

Division thm: let $z, a \in \mathbb{Z}[i]$, $a \neq 0$. Then there exists $\underset{\mathbb{Z}[i]}{q}, r$

s.t.: $z = qa + r$, $|r| < |a|$.

Pf: Consider $\frac{z}{a}$ in $\mathbb{Q}(i) = \{a+bi \mid a, b \in \mathbb{Q}\}$

say $\frac{z}{a} = \alpha + \beta i$ let $x, y \in \mathbb{Z}$ be closest to α, β so

$|x-\alpha|, |x-\beta| \leq \frac{1}{2}$

set $q = x + iy$ then $\left|\frac{z}{a} - q\right|^2 = |(\alpha+\beta i) - (x+iy)|^2$

$= |(\alpha - x) + (\beta - y)i|^2 = (\alpha-x)^2 + (\beta-y)^2$

$\leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1$

so $N\left(\frac{z}{a} - q\right) < 1$

so $N(z - qa) < Na$

Def: $\gcd(z,w)$ = any number of largest norm dividing both z, w.

(exists since if $d|z$, $Nd \mid Nz$, so $Nd \le Nz$)

<u>Euclid's algorithm</u> still works (with division steps)

<u>Thm</u>: $\forall z, w\ \exists x, y$ s.t. $\gcd(z,w) = x \cdot z + yw$

<u>Pf</u>: let $I = \{ x \cdot z + y \cdot w \mid x, y \in \mathbb{Z}[i] \}$

if $z = w = 0$, then $I = \{0\} = 0$, $0 = \gcd(0,0)$ done

else, I has non-zero members. let $d \in I$ have least norm $\neq 0$

certainly, d has the form $d = x \cdot z + yw$ for some $x, y \in \mathbb{Z}[i]$

Also, $d|z$, $d|w$: by division thm, $z = qd + r$ for some q, r

$|r| < |d|$. Then

$$r = z - qd = z - q(xz + yw)$$
$$= (1 - qx) \cdot z + (-qy) \cdot w \in I$$

but $|r| < |d|$, so $Nr = 0$, so $d|z$. same for $d|w$.

$d \in I$ has <u>least</u> non-zero norm

$\Rightarrow d$ is a common divisor.

But every common divisor of z, w divides $xz + yw = d$

so d is <u>largest one</u>.

What about order p, $2p$?

~~If~~ $\text{Ord}_q(a^2) = \dfrac{\text{ord}_q(a)}{(2, \text{ord}_q(a))}$

so if $\text{ord}_q(a) = 2p$, $\text{ord}_q(a^2) = p$

if $\text{ord}_q(a) = p$, $\text{ord}_q(a^2) = p$

So all squares (other than 1) have order p

(note: -1 not a square mod q, since $p \equiv 1 (2) \Rightarrow 2p \equiv 2 (4)$
$\Rightarrow 2p+1 \equiv 3 (4)$)

or: suppose $x^2 \equiv -1 (q)$. Then $x^4 \equiv 1 (q)$ but $\text{ord}_q(x) \nmid 2$ so $\text{ord}_q(x) = 4$
but no such x exists)

Conversely, if a mod q is a square (= quadratic residue)
then $\text{ord}_q(a) = p$. (or 1 if $a \equiv 1 (q)$)

Indeed, say $a \equiv r^\ell$ where r is a primitive root.

a is a square iff $a \equiv b^2$ mod q, i.e. iff $\ell \equiv 2k \ (\phi(q))$
$(b \equiv r^k)$ or iff $\ell \equiv 2k \ (2p)$

this has a solution k, iff ℓ is even. iff a is a square

when ℓ is even (but not 0 mod $2p$), $\underbrace{\text{ord}_q(r^\ell)}_{\text{ord}_q(a)} = \dfrac{2p}{\underbrace{2}_{2 = \gcd(\ell, 2p)}} = p$

Def: Call $\pi \in \mathbb{Z}[i]$ prime if $N\pi \geq 2$, & if $\pi | ab$ then $\pi | a$ or $\pi | b$

Easy: π prime $\Rightarrow$ π irreducible: $\pi = ab$ then $\pi | ab$
then if $\pi | a$ then $N\pi \leq Na \leq Na \cdot Nb \leq N\pi$ so $Nb = 1$
(mirror image if $\pi | b$)

Thm π irred $\Rightarrow$ π prime

Pf: Say $\pi | ab$ but $\pi \nmid a$. Then $\gcd(\pi, a) = 1$ (must divide π but isn't π)

By Bezout, $\exists x, y$: $x\pi + ya = 1$
then $x\pi b + yab = b$
but $\pi | x\pi b$, $\pi | ab$ so $\pi | xb\pi + yab = b$

(different view: ~~use~~ if $\pi \nmid a$, then a is invertible mod π,
so if $ab \equiv 0\ (\pi)$ then $b \equiv a\bar{a}b \equiv 0\ (\pi)$)

$\Rightarrow$ thm on unique factorization (same pf)
(except $\pi, -\pi, i\pi, -i\pi$ are same prime)

Modular arithmetic: works same way.

Non-obvious: Exactly $N\pi$ congruence classes mod π

If π is prime have primitive roots mod π.

Counter-example: in $\mathbb{Z}[\sqrt{7}]$: $\{a+b\sqrt{7}\}$

$2\cdot 3 = (\sqrt{7}+1)(\sqrt{7}-1)$