Math 310

Handy facts for the second exam

Don't forget the handy facts from the first exam!

Fermat's Little Theorem. If p is prime and $(a,p)=1$, then $a^{p-1} \underset{p}{\equiv} 1$

Because: $(a\cdot 1)(a\cdot 2)(a\cdot 3)\cdots(a\cdot(p-1)) \underset{p}{\equiv} 1\cdot 2\cdot 3\cdots(p-1)$, and $(1\cdot 2\cdot 3\cdots(p-1),p)=1$.

Same idea, looking at the a's between 1 and $n-1$ that are relatively prime to n (and letting $\phi(n)$ be the number of them), gives

If $(a,n)=1$, then $a^{\phi(n)} \underset{n}{\equiv} 1$.

$\phi(n)=n-1$ only when n is prime. Numbers n which are *not* prime but for which $a^{n-1} \underset{n}{\equiv} 1$ are called *a-pseudoprimes*; they are very uncommon!

One approach to calculating a^k (mod n) quickly is to start with a, and repeatedly square the result (mod n), computing $a^1, a^2, a^4, a^8, a^{16}$. etc. , continuing until the resulting exponent is more than half of k . a^k is then the product of some subset of our list - we essentially use the powers whose exponents are part of the base 2 expansion of k.

Rings. Basic idea: find out what makes our calculations in $\mathbb{Z}_n$ work.

A ring is a set R together with two operations $+,\cdot$ (which we call addition and multiplication) satisfying:

For any $r,s,t\in R$,

(0) $r+s, r\cdot s\in R$ [closure]
(1) $(r+s)+t=r+(s+t)$ [associativity of addition]
(2) $r+s=s+r$ [commutativity of addition]
(3) there is a $0_R\in R$ with $r+0_R=r$ [additive identity]
(4) there is a $-r\in R$ with $r+(-r)=0_R$ [additive inverse]
(5) $(r\cdot s)\cdot t=r\cdot(s\cdot t)$ [associativity of multiplication]
(6) there is a $1_R\in R$ with $r\cdot 1_R=1_R\cdot r=r$ [mutliplicative identity]
(7) $r\cdot(s+t)=r\cdot s+r\cdot t$ and $(r+s)\cdot t=r\cdot t+s\cdot t$ [distributivity]

These are the most basic properties of the integers mod n that we used repeatedly. Some others acquire special names:

A ring $(R,+,\cdot)$ satisfying: for every $r,s\in R$, $r\cdot s=s\cdot r$ is called *commutative.*

A commutative ring R satisfying if $rs=0_R$, then $r=0_R$ or $s=0_R$ is called an *integral domain.*

A ring R satisfying if $r\neq 0_R$, then $r\cdot s=s\cdot r=1_R$ for some $s\in R$ is called a *division ring.*

A commutative division ring is called a *field.*

An element $r\in R$ satisfying $r\neq 0_R$ and $r\cdot s=0_R$ for some $b\neq 0_R$ is called a *zero divisor.*

An element $r\in R$ satisfying $rs=sr=1_R$ for some $s\in R$ is called a *unit.*

An *idempotent* is an element $r\in R$ satifying $r^2=r$.

A *nilpotent* is an element $r\in R$ satisfying $r^k=0_R$ for some $k\geq 1$.

Examples: The integers $\mathbb{Z}$, the integers mod n $\mathbb{Z}_n$, the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$;

If R is a ring, then the set of all polynomials with coefficients in R, denoted $R[x]$, is a ring, where you add and multiply as you do with "ordinary" polynomials:

$R[x]=\{\sum_{i=0}^{n} r_r x^i : r_i\in R\}$ and (filling in with 0_R's as needed)

$$\sum_{i=0}^{n} r_r x^i + \sum_{i=0}^{m} s_r x^i = \sum_{i=0}^{n}(r_r+s_i)x^i \text{ and } \sum_{i=0}^{n} r_r x^i \cdot \sum_{j=0}^{m} s_r x^j = \sum_{k=0}^{n+m}(\sum_{i+j=k} r_i\cdot s_j)x^k$$

If R is a ring and $n \in \mathbb{N}$, then the set $M_n(R)$ of $n \times n$ matrices with entries in R is a ring, with entry-wise addition and 'matrix' multiplication:

the (i,j)-th entry of $(r_{ij}) \cdot (s_{ij})$ is $\displaystyle\sum_{k=0}^{n} r_{ik} \cdot s_{kj}$

If R is commutative, then so is $R[x]$; if R is an integral domain, then so is $R[x]$. If $n \geq 2$, then $M_n(R)$ is not commutative.

A *subring* is a subset $S \subseteq R$ which, using the same addition and multiplication as in R, is also a ring.

To show that S is a subring of R, we need:

(1) if $s, s' \in S$, then $s + s', s \cdot s' \in S$
(2) if $s \in S$, then $-s \in S$
(3) there is something that acts like a 1 in S (this need not be 1_R ! But $1_R \in S$ is enough...)

The Cartesian product of two rings R, S is the set $R \times S = \{(r,s) : r \in R, s \in S\}$. It is a ring, using coordinatewise addition and multiplication: $(r,s) + (r',s') = (r+r', s+s')$, $(r,s) \cdot (r',s') = (r \cdot r', s \cdot s')$

Some basic facts:

A ring has only one "zero": if $x + r = r$ for some R, then $x = 0_R$
A ring has only one "one": if $xr = r$ for every r, then $x = 1_R$
Every $r \in R$ has only one additive inverse: if $r + x = 0_R$, then $x = -r$
$-(-r) = r$; $0_R \cdot r = r \cdot 0_R = 0_R$; $(-1_R) \cdot r = r \cdot (-1_R) = -r$

Every finite integral domain is a field; this is because, for any $a \neq 0_R$, the function $m_a : R \to R$ given by $m_a(r) = ar$ is one-to-one, and so by the Pigeonhole Principle is also onto; meaning $ar = 1_R$ for some $r \in R$.

If R is finite, then every $r \in R$, $r \neq 0_R$, is either a zero-divisor or a unit (and can't be both!). Idea: The first time the sequence $1, r, r^2, r^3, \cdots$ repeats, we either have $r^n = 1 = r(r^{n-1})$ or $r^n = r^{n+k}$, so $r(r^{n+k-1} - r^{n-1}) = 0$.

A unit in $R \times S$ consists of a pair (r,s) where each of r, s is a unit. (The same is true for idempotents and nilpotents.)

For $n \in \mathbb{N}$ and $r \in R$, we define $n \cdot x = x + \ldots + x$ (add x to itself n times) and $x^n = x \cdot \cdots \cdot x$ (multiply x by itself n times). And we define $(-n) \cdot x = (-x) + \cdots + (-x)$. Then we have
$(n+m) \cdot r = n \cdot r + m \cdot r$, $(nm) \cdot r = n \cdot (m \cdot r)$, $r^{m+n} = r^m \cdot r^n$, $r^{mn} = (r^m)^n$

Homomorphisms and isomorphisms

A *homomorphism* is a function $\varphi : R \to S$ from a ring R to a ring S satisfying:
for any $r, r' \in R$, $\varphi(r + r') = \varphi(r) + \varphi(r')$ and $\varphi(r \cdot r') = \varphi(r) \cdot \varphi(r')$.

The basic idea is that it is a function that "behaves well" with respect to addition and multiplication.

An *isomorphism* is a homomorphism that is both one-to-one and onto. If there is an isomorphism from R to S, we say that R and S are *isomorphic*, and write $R \cong S$. The basic idea is that isomorphic rings are "really the same"; if we think of the function φ as a way of identifying the elements of R with the elements of S, then the two notions of addition and multiplication on the two rings are identical. For example, the ring of complex numbers $\mathbb{C}$ is isomorphic to a ring whose elements are the Cartesian product $\mathbb{R} \times \mathbb{R}$, provided we use the multiplication $(a,c) \cdot (c,d) = (ac - bd, ad + bc)$. And the main point is that anything that is true of R (which depends only on its properties as a ring) is also true of anything isomorphic to R, e.g., if $r \in R$ is a unit, and φ is an isomorphism, then $\varphi(r)$ is also a unit.

The phrase "is ismorphic to" is an equivalence relation: the composition of two isomorphisms is an isomorphism, and the inverse of an isomorphism is an isomorphism.

A more useful example: if $(m,n) = 1$, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. The isomorphism is given by

$\varphi([x]_{mn}) = ([x]_m, [x]_n)$

The main ingredients in the proof:

If $\varphi : R \to S$ and $\psi : R \to T$ are ring homomorphisms, then the function $\omega : R \to S \times T$ given by $\omega(r) = (\varphi(r), \psi(r))$ is also a homomorphism.

If $m|n$, then the function $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$ given by $\varphi([x]_n) = [x]_m$ is a homomorphism.

Together, these give that the function we want above is a homomorphism. The fact that $(m, n) = 1$ implies that φ is one-to-one; then the Pigeonhole Principle implies that it is also onto!

The above isomorphism and induction imply that if $n_1, \dots n_k$ are *pairwise relatively prime* (i.e., if $i \neq j$ then $(n_i, n_j) = 1$), then

$\mathbb{Z}_{n_1 \cdots n_k} \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$. This implies:

The Chinese Remainder Theorem: If $n_1, \dots n_k$ are pairwise relatively prime, then for any $a_1, \dots a_k \in \mathbb{N}$ the system of equations

$x \equiv a_i \pmod{n_i}$, $i = 1, \dots k$

has a solution, and any two solutions are congruent modulo $n_1 \cdots n_k$.

A solution can be found by (inductively) replacing a pair of equations $x \equiv a \pmod{n}$, $x \equiv b \pmod{m}$, with a single equation $x \equiv c \pmod{nm}$, by solving the equation $a + nk = x = b + mj$ for k and j, using the Euclidean Algorithm.

Application to units and the Euler ϕ-function:

If R is a ring, we denote the units in R by R^* . E.g., $\mathbb{Z}_n^* = \{[x]_n \ ; \ (x, n) = 1\}$. From a fact above, we have $(R \times S)^* = R^* \times S^*$.

$\phi(n)$ = the number of units in $\mathbb{Z}_n = |\mathbb{Z}_n^*|$; then the CRT implies that if $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(m)$. Induction and the fact that if p is prime $\phi(p^k) = p^{k-1}(p-1) = p^k -$(the number of multiples of p) implies

If the prime factorization of n is $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then $\phi(n) = [p_1^{\alpha_1 - 1}(p_1 - 1)] \cdots [p_k^{\alpha_k - 1}(p_k - 1)]$

Groups: Three important properties of the set R^* of units of a ring R:

$1_R \in R^*$

if $x, y \in R^*$, then $xy \in R^*$

if $x \in R^*$ then (x, by definition, has a multiplicative inverse x^{-1} and) $x^{-1} \in R^*$

Together, these three properties (together with associativity of multiplication) describe what is called a *group*.

A *group* is a set G together with a single operation (denoted $*$) satisfying:

For any $g, h, k \in G$,

(0) $g * h \in G$ [closure]

(1) $g * (h * k) = (g * h) * k$ [associativity]

(2) there is a $1_G \in G$ satisfying $1_G * g = g * 1_G = g$ [identity]

(3) there is a $g^{-1} \in G$ satisfying $g^{-1} * g = g * g^{-1} = 1_G$ [inverses]

A group $(G.*)$ which, in addition, satisfies $g * h = h * g$ for every $g, h \in G$ is called *abelian*. Since this is something we always expect out of addition, if we know that a group is abelian, we often write the group operation as "+" to help remind ourselves that the operation commutes.

Examples: Any ring $(R, +, \cdot)$, if we just forget about the multiplication, is an (abelian) group $(R, +)$.

For any ring R, the set of units $(R^*, \cdot)$ is a group using the multiplication from the ring. [[Unsolved (I think!) question: is every group the group of units for some ring R?]]

Function composition is always associative, so one way to build many groups is to think of the elements as functions. But to have an inverse under function composition, a function needs to be both one-to-one <u>and</u> onto. [One-to-one is sometimes also called *injective*, and onto is called *surjective*; a function that is both injective and surjective is called *bijective*.] So if, for any set S, we set

$G = P(S) = \{f : S \to S : f$ is one-to-one and onto$\}$,

then G is a group under function composition; it is called the group of *permutations* of S. If S is the finite set $\{1, 2, \ldots, n\}$, then we denote the group by S_n, the *symmetric group on n letters*. By counting the number of bijections from a set with n elements to itself, we find that S_n has $n!$ elements.

The set of rigid motions of the plane, that is, the functions $f : \mathbb{R}^2 \to \mathbb{R}^2$ satisfying $\text{dist}(f(x), f(y)) = \text{dist}(x, y)$ for every $x, y \in \mathbb{R}^2$, is a group under function composition, since the composition or inverse of rigid motions are rigid motions. More generally, for any geometric object T (like a triangle, or square, or regular pentagon, or...), the set of rigid motions f which take T to itself form a group, the group $\text{Symm}(T)$ of *symmetries* of T. For example, for $T =$ a square, $\text{Symm}(T)$ consists of the identity, three rotations about the center of the square (with rotation angles $\pi/2, \pi,$, and $3\pi/2$), and four reflections (through two lines which go through opposite corners of the square, and two lines which go through the centers of opposite sides).

$G = \text{Aff}(\mathbb{R}) = \{f(x) = ax + b : a \neq 0\}$, the set of linear, non-constant functions from $\mathbb{R}$ to $\mathbb{R}$, form a group under function composition, since the composition of two linear functions is linear, and the inverse of a linear function is linear. It is called the *affine group of* $\mathbb{R}$. This is an example of a *subgroup* of $P(\mathbb{R})$:

A *subgroup* H of G is a subset $H \subseteq G$ which, using the same group operation as G, is a group in its own right. As with subrings, this basically means that:

(1) If $h, k \in H$, then $h * k \in H$
(2) If $h \in H$, then $h^{-1} \in H$
(3) $1_G \in H$.

Condition (3) really need not be checked (so long as $H \neq \emptyset$), since, for any $h \in H$, (2) guarantees that $h^{-1} \in H$, and so (1) implies that $h * h^{-1} = 1_G \in H$.

For example, for the symmetries of a polygon T in the plane, since a symmetry must take the corners of T (called its *vertices*) to the corners, each symmetry can be thought of as a permutation of the vertices. So $\text{Symm}(T)$ can be thought of (this can be made precise, using the notion of isomorphism below) as a subgroup of the group of symmetries of the set of vertices of T.

As with rings, some basic facts about groups are true:

There is only one "one" in a group; if $x \in G$ satisfies $x * y = y$ for some $y \in G$, then $x = 1_G$

Every $g \in G$ has only one inverse: if $g * h = 1_G$, then $h = g^{-1}$

$(g^{-1})^{-1} = g$ for every $g \in G$

$(gh)^{-1} = h^{-1}g^{-1}$

Homomorphisms and isomorphisms: Just as with rings, again, we have the notion of functions between groups which "respect" the group operations:

A *homomorphism* is a function $\varphi : G \to H$ from groups G to H which satisfies:

for every $g_1, g_2 \in G$, $\varphi(g_1 * g_2) = \varphi(g_1) * \varphi(g_2)$

No other condition is required, since this <u>implies</u> that

$\varphi(1_G) = 1_H$,as well as $\varphi(g^{-1}) = (\varphi(g))^{-1}$.

An *isomorphism* is a homomorphism that is also one-to-one and onto. If there is an isomorphism from G to H, we say that G and H are *isomorphic*. As with rings, the idea is that ismorphic groups are really the "same"; the function is a way of identifying elements so that the two groups are identical (as groups!). For example, the group $\text{Aff}(\mathbb{R})$ can be thought of as $\mathbb{R} \times \mathbb{R}$ (i.e., the pair of coefficients of the linear function), but with the group multiplication given by (by working out what the coeffiicients of the composition are!) $(a, b) * (c, d) = (ac, ad + b)$.