Notes for 6 March (Wednesday)

1 The road so far...

1. Stated the Diffey-Hellman protocol and the RSA algorithm. (BTW RSA works because m is squarefree. I forgot to mention this.)

2. Stated and proved the Chinese Remainder Theorem.

2 The Chinese Remainder theorem

We shall use the Chinese Remainder theorem to prove properties about $\phi(m)$. Before we do so, here is a proposition that is sort of a converse to what we did earlier.

Theorem 1. *Every ring homomorphism $g : \mathbb{Z}/m\mathbb{Z} \to S$ where S is a commutative ring "lifts" to a ring homomorphism $f : \mathbb{Z} \to S$ so that $m\mathbb{Z} \in ker(f)$. ("Lifts" means that g is induced from f in the way we studied earlier.)*

Proof. Define $f(n) = g([n])$. This map is a composition of homomorphisms and is hence a homomorphism. The kernel property is obviously satisfied. □

Now we define a useful way to construct new rings out of old ones. Suppose $(R, 0_R, 1_R, +_R, ._R)$ and $(S, 0_S, 1_S, +_S, ._S)$ are two rings. Then we can define a ring structure on $R \times S$ as follows : $0_{R\times S} = (0_R, 0_S)$, $1_{R\times S} = (1_R, 1_S)$, $(a, b) +_{R\times S} (c, d) := (a +_R c, b +_S d)$, $(a, b)._{R\times S}(c, d) = (a._R c, b._S d)$, $-(a, b) = (-a, -b)$. It can be easily verified that these operations define a ring. In fact, here is a way to construct a group $G \times H$ out of two groups G, H : $(a, b) * (c, d) = (a * b, c * d), e_{G\times H} = (e_G, e_H)$. Note however, that the product of fields is not a field ! If R, S are commutative, then so is $R \times S$ (and likewise for groups). Here is a proposition about products.

Lemma 2.1. *1. (a, b) is a unit in $R \times S$ iff a is a unit in R and b is a unit in S.*

2. (a, b) is a zero divisor iff $(a, b) \neq (0, 0)$ and either a is 0 or a zero-divisor, or b is 0 or a zero-divisor.

Proof. The first part is trivial. For the second part, if R is not commutative, (a, b) is a left (likewise, right) zero divisor iff it is not zero and there exists a non-zero (c, d) such that $(a, b).(c, d) = (0, 0)$ (likewise $(c, d).(a, b) = (0, 0)$). W.LOG assume it is a left zero divisor. This observation means that $a.c = 0$ and $b.d = 0$. Hence either $a = 0$ or a zero divisor and likewise for b. □

As a corollary,

Lemma 2.2. *If R, S are commutative rings whose groups of units are U_R, U_S, then $U_{R\times S} = U_R \times U_S$ via the identity map.*

Here is a very important theorem (which is basically equivalent to the Chinese Remainder theorem).

Theorem 2. *Let $m = rs$ where r, s are coprime natural numbers ≥ 2. Then there is an isomorphism of rings $\psi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}_r \times \mathbb{Z}_s$ given by $\psi([a]_m) = ([a]_r, [a]_s)$.*

Proof. This map is well-defined because r, s divide m. We need to prove that it is $1-1$ and onto. Now, the kernel consists of a such that $a = rk_1 = sk_2$ and hence $a = lcm(r,s)k_3 = rsk_3$ which means that $[a]_m = 0$. So it is $1-1$. If $([x]_r, [y]_s)$ is in the codomain, we need to prove that there is an a such that $a = x + rk_1$ and $a = y + sk_2$. By the Chinese Remainder Theorem, such an exists and is unique upto m. Alternatively, a $1-1$ map between sets of the same finite cardinality is onto. □

This theorem provides an alternate method of solving $x \equiv_r b$ and $x \equiv_s c$. Indeed, suppose e_1 solves, $e_1 \equiv_r 1$ and $e_1 \equiv_s 0$, then $\psi(e_1) = (1, 0)$. Likewise, there is an e_2 such that $\psi(e_2) = (0, 1)$. Thus, $\psi(be_1 + ce_2) = (b, c)$ which is what we wanted. The Chinese Remainder theorem in the above form leads us to prove an important result and a corollary.

Theorem 3. *If $m = rs$, and $gcd(r, s) = 1$, then $\psi : \mathbb{Z}_m \to \mathbb{Z}_r \times \mathbb{Z}_s$ given as above is an isomorphism between the groups of units U_m and $U_r \times U_s$.*

Proof. Note that the ring isomorphism ψ induces a group homomorphism between the groups of units. Likewise, the inverse of the ring isomorphism also induces a group homomorphism in the other direction, which is an inverse of the previous group homomorphism. □

As a corollary,

Theorem 4. *If $m = rs$ and $gcd(r, s) = 1$, then $\phi(m) = \phi(r)\phi(s)$.*

Using induction, $\phi(m) = \Pi_i \phi(p_i^{e_i})$.

3 Polynomials

Definition of a polynomial $p(x)$ of degree with coefficients in a commutative ring R : It is an element of the set R^{d+1} written as $p(x) = a_0 + a_1 x + \ldots a_d x^d$. The set of polynomials is denoted as $R[x] = \cup_{d\geq 0} R^{d+1}$. This set is much better written as R^∞ where all but finitely many elements are 0. $R[x]$ has a ring operation defined as follows : $1 := (1, 0, 0 \ldots)$ is the multiplicative identity, $0 := (0, 0, 0 \ldots)$ is the additive identity. Addition is componentwise. Multiplication is defined as $(a_0, \ldots, a_{d_1}, 0, 0 \ldots).(b_0, \ldots, b_{d_2}, 0, 0 \ldots) = (a_0 b_0, a_0 b_1 + a_1 b_0, \ldots, \sum_{i=0}^{d_1 d_2} a_i b_{k-i}, 0, 0, \ldots)$. It can be easily proven that multiplication makes it into a commutative monoid and distributivity holds. Hence $R[x]$ is a commutative ring. The variable x is identified with $(0, 1, 0 \ldots)$.