Math 152 Notes

Lucas Garron

September 30, 2009

20090929

Statement 1: If $(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \bmod p$.
Statement 2: $a^p \equiv a \bmod p$.
Note $S1 \Rightarrow S2$
$(a + b, \frac{a^p+b^p}{a+b}) = 1, p$

BINOMIAL THEOREM: $\binom{a}{b} = \frac{a!}{b!(a-b)!}, 0 \leq b \leq a$
$\binom{a}{b} = 0$ if $b = 0$ or $b > a$
$(\binom{a}{b} = \frac{a!}{b!(a-b)!} \in Z)$
Observe if p is prime $1 \leq a \leq p - 1$
Then $\binom{a}{b}$ is a multiple of p because $\binom{p}{a} = \frac{p!}{a!(p-a)!}$. p divides numerator, but not denom.
If $2 \leq a \leq p - 1 \Rightarrow p$ divides $\binom{p+1}{a}$

THM: $(a + b)^p = a^p + b^p \bmod p$. (Fermat's Theorem: both sides $\equiv a + b \bmod p$)
Because: The Binomial Theorem $(a + b)^p = a^p + \binom{p}{1} a^{p-1} b + ... + b^p$ and each term but first and last has factor p.

Important fact: $(x + y)^p \equiv x^p + y^p$ mod p if p prime.

Thm (Fermat): $x^p \equiv x$ mod p.
Proof by induction on $0 \leq x \leq Z$.
$x = 0$, trivial. If true for x, i.e. $x^p \equiv x$ then $(x + 1)^p \equiv x^p + 1^p \equiv x + 1$ (Induction.)

Integers mod m form a ring. (Denoted Z_m in book. Z/mZ more universal.)
Notation: $a \equiv b \bmod m$ means a-b is a mult of m.
Key fact: If $a \equiv a'$ mod m and $b \equiv b'$ mod m $\Rightarrow a + b \equiv a' + b'$ mod m and $ab\ a'b'$ mod m.
$ab - a'b' = a(b - b') + (a - a')b' \equiv 0$ (implies addition and multiplication mod m are well-defined, see below).

Let us define $\bar{a} = \{x \in R | a \equiv a \bmod m\}$ the residue classes mod m. There are m residue classes.

m=3:

$\bar{0} = \{0, \pm 3, \pm 6, ...\}$
$\bar{1} = \{1, 4, 7, ..., -2, -5, ...\}$
$\bar{2} = \{2, 5, 8, ..., -1, -4, -7\}$

D efine a ring structure on Z_n = these residue classes.
$\bar{a} + \bar{b} = \overline{a + b}$, $\bar{a}\bar{b} = \overline{ab}$
A commutative ring is a field if $0 \neq x \in F \Rightarrow \exists y$ with $xy = yx = 1$, i.e. all nonzero elements are units.
Q, C, R are fields, Z is not.

If p is a prime, Z_p is a field.
Proof: If $\bar{a} \neq 0$ this means $a \not\equiv 0$ mod p, (a, p)=1. Implies $\exists m, n 1 = ma + np$. $\bar{1} = \bar{m}\bar{a} \Rightarrow \bar{a}^{-1}$ $\bar{m}$ in Z_p

Galois proved: If q is prime power $q = p^k$ some prime p $\Rightarrow \exists$ finite field $GF(q) = F_q$ with q elements.
If q is not prime, $GF(q) \neq Z_q$ (different rings).
In $GF(q)$ if $q = p^k$ in that case $x^p \neq x$
$p = 2$, $(\alpha^2 + \beta)^2 = 1 = \alpha^2 + \beta^2$

Other proof of Fermat's theorem:
$\phi(m)$ = Euler's totient function = # of units in Z_m = # of residue classes mod m prime to m. (These defs are equiv. since $\bar{a}$ is a unit $\Leftrightarrow (a, m) = 1$)

Fact: $\phi(p^k) = p^k - p^{k-1}$, p prime, k¿0
If$(a, b) = 1$ then $\phi(ab) = \phi(a)\phi(b)$: ϕ is "multiplicative." (Proof Thursday.)
$\phi(100)$

Thm (Euler): If $(a, m) = 1$ then $a^{\phi(m)} \equiv 1$ mod m
Note: If $m = p$, $\phi(p) = p - 1$, so this reduces to Fermat's Theorem.

Z_p Fermat Generalizations:
$\rightarrow Z_m$: Euler (residue fields) $\rightarrow GF(q)$: Galois. (Frobenius map $F(x) = x^p$, $F(xy) = F(x)F(y)$, $F(x + y) = F(x) + F(y)$) Proof from Last Thursday will adapt.