Supplement 3: Fields and Polynomials.

1. Definitions and basic theorems.

Recall that we have used the term *ring* for a set R with two binary operations $+$ and $\cdot$ satisfying:

R-1 (Commutativity) $a+b=b+a, a\cdot b=b\cdot a$ for $a,b\in R$.

R-2 (Associativity) $a+(b+c)=(a+b)+c,\ a\cdot(b\cdot c)=(a\cdot b)\cdot c$ for $a,b,c\in R$.

R-3 (Distributive Rule) $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$.

R-4 There exist elements $0,1\in R$ such that $a+0=a$ and $a\cdot 1=a$ for all $a\in R$.

R-5 If $a\in R$ there exists $b\in R$ such that $a+b=0$.

In the literature this is called a *commutative ring with unit.* Since this is the main type of ring that will occur in this course we will continue to call such an object a ring. We have seen that R-2 allows us to write expressions like $a+b+c+d$ or $a\cdot b\cdot c\cdot d$ without regard for how to put in the parentheses. We have shown that R-4 uniquely specifies $0,1$ and in R-5 given a there is a unique b such that $a+b=0$ and we have denoted it $-a$.

Our main examples have been $\mathbb{Z},\mathbb{R},\mathbb{C},\mathbb{Q}$ with the usual multiplication and addition and in addition for every $m\in\mathbb{Z}_{>0}$ the ring $\mathbb{Z}/m\mathbb{Z}=\{0,1,...,m-1\}$ with addition $+_m$ and $\cdot_m$ given by

$$a+_m b, a\cdot_m b\in\{0,1,...,m-1\}$$

with

$$a+b\equiv a+_m b \bmod m, ab\equiv a\cdot_m b \bmod m.$$

We note that if we have a ring R then we can construct a new ring by considering polynomials in an indeterminate, t, with coefficients in R. That is expressions:

$$f(t)=a_0+a_1t+a_2t^2+...+a_nt^n$$

with $a_0,...,a_n\in R$. Here if

$$g(t)=b_0+b_1t+b_2t^2+...+b_mt^m$$

then we say $f(t)=g(t)$ if when we write $b_i=0$ for $m<i\leq\max(m,n)$ and $a_j=0$ for $n<j\leq\max(m,n)$ then $a_i=b_i$ for all $0\leq i\leq\max(m,n)$ (we call this procedure *extension by* 0). Thus $1+t+t^2=1+t+t^2+0t^3$.

We denote the set of polynomials with coefficients in R in the indeterminate t with this notion of equality by $R[t]$. We make this set into a ring as follows:

0 is the polynomial *with* all coefficients 0 and 1 is the polynomial with $a_0 = 1$ and all other coefficients 0 we note that for example $0 = 0 + 0t + 0t^2$ and $1 = 1 + 0t$.

If $f(t)$ and $g(t)$ are as above and extended by 0 then

$$f(t) + g(t) = (a_0 + b_0) + (a_1 + b_1)t + ... + (a_{\max(m,n)} + b_{\max(m,n)})t^{\max(m,n)}$$

and

$$f(t) \cdot g(t) = (a_0 b_0) + (a_0 b_1 + a_1 b_0)t + ... + (a_0 b_r + a_1 b_{r-1} + ... + a_{r-1} b_1 + a_r b_0)t^r + ... + a_n b_m t^{n+m}$$

here if $r > n$ we set $a_r = 0$ and if $r > n$ we set $b_r = 0$.

Examples. In $\mathbb{Z}[t]$, we have $(1 + 3t)(1 + 2t + 5t^2) =$

$$1 + (1 \cdot 2 + 1 \cdot 3)t + (1 \cdot 5 + 3 \cdot 2 + 0 \cdot 1)t^2 + (1 \cdot 0 + 3 \cdot 5 + 0 \cdot 2 + 0 \cdot 1)t^3 =$$

$$1 + 5t + 11t^2 + 15t^3.$$

In $\mathbb{Z}/6\mathbb{Z}$ we have $(1 + 3t)(1 + 2t + 5t^2) =$

$$1 + (1 \cdot_6 2 + 1 \cdot_6 3)t + (1 \cdot_6 5 + 3 \cdot_m 2 + 0 \cdot_6 1)t^2 + (1 \cdot_6 0 + 3 \cdot_6 5 + 0 \cdot_6 2 + 0 \cdot_6 1)t^3$$

$$= 1 + 5t + 5t^2 + 3t^3.$$

If we are calculating in $\mathbb{Z}/m\mathbb{Z}$ and m is understood then we will omit the subscript m.

Definition 1 *If $f(t) = a_0 t^0 + a_1 t^1 + a_2 t^2 + ... + a_n t^n$ is not equal to 0 then we define $\deg f(t) = \max\{j | a_j \neq 0\}$ and call this number the degree of $f(t)$. If $f(t) = 0$ meaning all of the $a_j = 0$ then $\deg f(t) = -1$. If $f(t) \neq 0$ is of degree n, that is $a_n \neq 0$ then we call a_n its leading coefficient. We say that $f(t)$ is monic if $a_n = 1$.*

Example: $\deg(1 + 3t + 7t^2 + t^7 + 0t^{15}) = 7$, $\deg 1 = 0$.

If $f(t) = a_0 t^0 + a_1 t^1 + a_2 t^2 + ... + a_n t^n \in R[t]$, then if $r \in R$ we set $f(r) = a_0 + a_1 r^1 + a_2 r^2 + ... + a_n r^n$.

Definition 2 *If $f(t) \in R[t]$ then $a \in R$ is called a root of $f(t)$ if $f(a) = 0$.*

Example: -1 is a root of $-1+3t+7t^2+3t^7$ if we look at this polynomial with coefficients in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{Z}/m\mathbb{Z}$ (with the understanding that we reduce modulo m).

Proposition 3 *If R is a ring and if t is an indeterminate then $R[t]$ is a ring.*

Proof. All of the conditions in R-1,2,3,4,5 having to do with addition are satisfied since addition is coefficientwise. The commutative rule for multiplication follows from

$$a_0b_r + a_1b_{r-1} + ... + a_{r-1}b_1 + a_rb_0 =$$

$$b_ra_0 + b_{r-1}a_1 + ... + b_1a_{r-1} + b_0a_r =$$

$$b_0a_r + b_1a_{r-1} + ... + b_{r-1}a_1 + b_ra_0.$$

A direct proof of the associative rule is complicated. We note that the distributive rule is simpler and we will leave it to the student.

We now note that we can rewrite

$$f(t)g(t) = a_0g(t) + a_1tg(t) + ... + a_mt^mg(t)$$

and

$$(a_jt^j)g(t) = a_jb_0t^j + a_jb_1t^{j+1} + ... + a_jb_mt^{j+m}.$$

If $c_k \in R$ then

$$(c_kt^k)((a_jt^j)g(t))) = (c_kt^k)(a_jb_0t^j + a_jb_1t^{j+1} + ... + a_jb_mt^{j+m}) =$$

$$c_ka_jb_0t^{k+j} + c_ka_jb_1t^{k+j+1} + ... + c_ka_jb_mt^{k+m+j} =$$

$$(c_ka_jt^{k+j})g(t) = ((c_kt^k)(a_jt^j))g(t)(*)$$

thus if $h(t) = c_0 + c_1t + ... + c_pt^p$ then we see that

$$h(t)(f(t)g(t)) = (h(t)f(t))g(t)$$

by expanding $h(t)$ and $g(t)$ and using $(*)$. ■

Lemma 4 *If $f(t)$ and $g(t)$ are monic polynomials of degree m and n respectively then* $\deg(f(t)g(t)) = n + m$.

Proof. This follows since the highest power of t that can have a nonzero coefficients is t^{n+m} and its coefficient is 1. ■

The examples $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ satisfy one additional condition

F-6 (Inverse) If $a \in R$ and $a \neq 0$ then there exists $b \in R$ such that $a \cdot b = 1$.

Notice that this is more restrictive than R-5 (the analogous condition for addition). We do not allow division by 0. As in the case of R-5 the element b in F-6 is uniquely determined by a. We denote it a^{-1} and use the notion $c/a = ca^{-1}$.

If F-6 is satisfied then we call R a *field.*

Theorem 5 *$\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is a prime.*

This is exactly the first part of problem 4 on the midterm exam.

We now come to the main reason for this supplement.

Theorem 6 *(Division algorithm for polynomials)Let F be a field. If $f(t)$ and $g(t) \in F[t]$ and $g(t) \neq 0$ then we can write*

$$f(t) = q(t)g(t) + r(t)$$

with $q(t) \in F[t]$ and $\deg r(t) < \deg g(t)$.

Proof. If $\deg f(t) < \deg g(t)$ take $q(t) = 0$ and $r(t) = f(t)$. We will now prove the result by induction on $\deg f(t)$. If $\deg f(t) = -1$ (base case -1) then $\deg f(t) < \deg g(t)$. Thus the base case is true. Assume that the result is true for polynomials of degree $< n$. We will now prove that this implies the result for $f(t)$ of degree $= n$. If $n < \deg g(t)$ then the result is true. Thus we may assume that $n \geq \deg g(t)$. Let a_n be the coefficient of t^n in $f(t)$, let $m = \deg g(t)$ and let b_m be the coefficient of t^m in $g(t)$. Set $h(t) = f(t) - \frac{a_n}{b_m} t^{n-m} g(t)$. The effect of this subtraction is to make the coefficient of t^n equal 0. Thus $\deg h(t) < n$. Hence the inductive hypothesis implies that there are polynomials $u(t)$ and $r(t)$ with $\deg r(t) < \deg g(t)$ such that

$$h(t) = u(t)g(t) + r(t).$$

Now $f(t) = h(t) + \frac{a_n}{b_m} t^{n-m} g(t) = u(t)g(t) + r(t) + \frac{a_n}{b_m} t^{n-m} g(t) = (u(t) + \frac{a_n}{b_m} t^{n-m})g(t) + r(t)$.Take $q(t) = u(t) + \frac{a_n}{b_m} t^{n-m}$. ■

We note that the method of proof gives a way (algorithm) to calculate $q(t)$ and $r(t)$.

Example. $f(t) = 5t^3 + 2t + 3$ and $g(t) = 2t^2 + 1$. Then $f(t) - \frac{5}{2}tg(t) = 5t^3 + 2t + 3 - (\frac{5}{2}t^3 + \frac{5}{2}t) = -\frac{1}{2}t + 3$. Thus $q(t) = \frac{5}{2}t$ and $r(t) = -\frac{1}{2}t + 3$. Note that we could not do this and stay in $\mathbb{Z}[t]$. It was necessary to find $q(t)$ and $r(t)$ in $\mathbb{Q}[t]$.

We say that a polynomial $g(t)$ *divides* $f(t)$ if there exists a polynomial $h(t)$ such that $f(t) = g(t)h(t)$. If $f(t)$ and $g(t)$ are polynomials in $R[t]$ then we say that $u(t)$ is a greatest common divisor (GCD) of $f(t)$ and $g(t)$ if $u(t)$ divides both $f(t)$ and $g(t)$ and if $v(t)$ divides $f(t)$ and $g(t)$ then $v(t)$ divides $u(t)$.

Lemma 7 *If $f(t)$ and $g(t)$ are monic polynomials in $F[t]$ with F a field then if $f(t)$ divides $g(t)$ and $g(t)$ divides $f(t)$ then $f(t) = g(t)$.*

Proof. The hypothesis says that $g(t) = u(t)f(t)$ and $f(t) = v(t)g(t)$. Thus $\deg g(t) = \deg u(t) + \deg f(t)$ and $\deg f(t) = \deg v(t) + \deg g(t)$ (Lemma 4). Thus $\deg g(t) \geq \deg f(t)$ and $\deg f(t) \geq \deg g(t)$. Thus $\deg f(t) = \deg g(t)$ and this implies that $\deg u(t) = 0$. Since $f(t)$ and $g(t)$ are monic this implies that $u(t) = 1$ hence $f(t) = g(t)$. ■

Theorem 8 *If F is a field and $f(t)$ and $g(t)$ are non-zero polynomials in $F[t]$ then they have a unique monic greatest common divisor $u(t)$. Furthermore, there exist polynomials $x(t), y(t)$ such that $u(t) = x(t)f(t) + y(t)g(t)$.*

Proof. Let $S = \{h(t)|h(t) = x(t)f(t) + y(t)g(t)$ with $x(t), y(t) \in F[t]\}$. We note that $f(t) \in S$ so $S \neq \{0\}$. Let $w(t)$ be a polynomial in S of lowest non-negative degree. If we divide $w(t)$ by its leading coefficient then we have a monic polynomial in S of minimal non-negative degree. $w(t) = x(t)f(t) + y(t)g(t)$. If $u(t)$ divides $f(t)$ and $g(t)$ then $f(t) = u(t)r(t)$ and $g(t) = u(t)p(t)$ thus $w(t) = x(t)r(t)u(t) + y(t)p(t)u(t) = (x(t)r(t) + y(t)p(t))u(t)$. So $u(t)$ divides $w(t)$. If $w(t)$ doesn't divide $f(t)$ then $f(t) = q(t)w(t) + r(t)$ with $r(t) \neq 0$ and $\deg r(t) < w(t)$. But then $r(t) = f(t) - q(t)w(t) = f(t) - q(t)x[t)f(t) - q(t)y(t)g(t) = (1 - q(t)x(t))f(t) + (-q(t)y(t))g(t)$. Thus $r(t)$ is non-zero in S and $\deg r(t) < \deg w(t)$. This is a contradiction. Thus $w(t)$ must divide $f(t)$. The same argument shows that $w(t)$ divides $g(t)$.

Suppose that $v(t)$ is a monic GCD for $f(t)$ and $g(t)$. Then $w(t)$ divides $v(t)$ and $v(t)$ divides $w(t)$. This implies by Lemma 7 that since both polynomials are monic they are equal. ■

Definition 9 *The monic GCD will be denoted* $\gcd(f(t), g(t))$. *If*

$$\gcd(f(t), g(t)) = 1$$

then we say that $f(t)$ *and* $g(t)$ *are relatively prime.*

Example. F is a field. If $f(t)$ and $g(t) \in F[t]$ are monic of degree 1 then $f(t) = g(t)$ or $\gcd(f(t), g(t)) = 1$. To see this we note that $f(t) - g(t)$ is of degree ≤ 0. If it is the 0 polynomial then $f(t) = g(t)$. Otherwise it is not 0 so as in the proof of the Theorem above $\gcd(f(t), g(t)) = 1$.

Theorem 10 *Let* F *be a field. If* $f(t)$ *and* $g(t) \in F[t]$ *are relatively prime polynomials and* $f(t)$ *divides* $g(t)u(t)$ *with* $u(t) \in F[t]$ *then* $f(t)$ *divides* $g(t)$.

Proof. We have $1 = x(t)f(t) + y(t)g(t)$ with $x[t], y(t) \in F[t]$. Thus $u(t) = x(t)u(t)f(t) + y(t)u(t)g(t)$. But $u(t)g(t) = f(t)z(t)$ with $z(t) \in F[t]$. Hence $u(t) = x(t)u(t)f(t) + y(t)f(t)z(t) = (x(t)u(t) + y(t)z(t))f(t)$. ■

Theorem 11 *Let* F *be a field. If* $f(t) \in F[t]$ *and* $a \in F$ *is a root of* $f(t)$ *then* $f(t)$ *is divisible by* $t - a$.

Proof. The division algorithm implies that $f(t) = q(t)(t - a) + r(t)$ with degree $r(t) < 1$. Thus $r(t) = c \in F$. Evaluating at $t = a$ yields $f(a) = q(a)(a - a) + c = c$. Thus $c = 0$. ■

Theorem 12 *Let* F *be a field. If* $f(t) \in F[t]$ *is of degree* $n > 0$ *and* $S = \{a \in F | f(a) = 0\}$ *then* S *has at most* n *elements.*

Proof. By induction on $\deg f(t)$. If the degree is 1 then if $f(t)$ has a root $a \in F$ then $f(t) = g(t)(t-a)$. $\deg g(t) = \deg f(t) - 1 = 0$. This $f(t) = c(t-a)$ with $c \in F, c \neq 0$. If $b \in F, b \neq a$ then $f(b) = c(b - a) \neq 0$ since F is a field. Thus $f(t)$ has at most one root. Assume the result is true for all polynomials of degree $n \geq 1$. Then if $\deg f(t) = n + 1$ and a is a root of $f(t)$ then $f(t) = (t - a)g(t)$ with $g(t)$ of degree n. If b is a root of $f(t)$ and $b \neq a$ then $f(b) = (b - a)g(b)$. This implies that $g(b) = 0$. thus a root of $f(t)$ is either a or a root of $g(t)$. Hence the inductive hypothesis implies that the number of roots of $f(t)$ is at most $n + 1$. ■

2.Number theoretic applications.

In this part of the supplement we will consider the case when our field is $\mathbb{Z}/p\mathbb{Z}$ with p a prime. We will use the more standard notation F_p.

We first consider the polynomial $f(t) = t^{p-1} - 1$. Then a restatement of Fermat's Little Theorem (using Theorem 12) is that the non-zero elements of F_p are exactly the roots of $f(t)$.

Lemma 13 *Let F be a field and let $a \in F$ be such that $a^n = 1$ for some $n > 0$ and $a \neq 1$. Then there exists $m > 1$ such that if $k \in \mathbb{Z}_{>0}$ and $a^k = 1$ then $m|k$. Furthermore,if $0 < k < m$ then $a^k \neq 1$.*

Proof. Let $S = \{k \in \mathbb{Z}_{>0} | a^k = 1\}$. Then $n \in S$. Thus well ordering implies that S has a minimal element, m. This element satisfies the last assertion. We note that $m \neq 1$ since $a \neq 1$. Let $k \in S$. Then $k = qm + r$ with $0 \leq r < m$ (division algorithm for $\mathbb{Z}$). By the definition of S we have $a^k = 1$. Thus $1 = a^{qm+r} = a^{qm}a^r = (a^m)^q a^r = a^r$ since $a^m = 1$. If $r \neq 0$ then we would contradict the definition of m. Thus $r = 0$ so $k = mq$. ■

Definition 14 *We will call the integer m in the above lemma the order of a. If $a = 1$ we will say that the order of a is 1 and if no $n \in \mathbb{Z}_{>0}$ exists such that $a^n = 1$ then we will say that a has infinite order.*

Lemma 15 *Let p be a prime. If $a \in F_p$ and $a \neq 0$ then a has finite order, m, dividing $p - 1$.*

Proof. Fermat's theorem implies that $a^{p-1} = 1$ in F_p. Thus we can apply the preceding lemma which implies that the order of a, m has the desired properties. ■

Lemma 16 *Assume that F is a field and $a \in F - \{0\}$ have order m. If $s \in \mathbb{Z}_{>0}$ then the order of a^s divides m.*

Proof. $(a^m)^s = 1^s = 1$. Since $(a^s)^m = (a^m)^s$, Lemma 13 implies that the order of a^s divides m. ■

Theorem 17 *Let p be a prime then there exists $a \in F_p - \{0\}$ such that $F_p - \{0\} = \{1, a, a^2, ..., a^{p-2}\}$. In other words there exists an element of $F_p - \{0\}$ of order $p - 1$.*

Proof. Let $a \in F_p - \{0\}$ be of maximal order, m. Assume that $m < p-1$. We consider the polynomial $f(t) = t^m - 1$. Then the powers $1, a, a^2, ..., a^{m-1}$ are all roots of $f(t)$. Thus Theorem 12 implies that $\{1, a, a^2, ..., a^{m-1}\}$ is exactly the set of roots of $f(t)$ in F_p. Let b be a nonzero element of F_p and assume that it is not a power of a. Let k be the order of b. Let $r = \gcd(m, k)$. By the definition of GCD $m = ur$ and $k = vr$ with $u, v \in \mathbb{Z}$. Then if we set $c = b^r$ then c has order v and $\gcd(v, m) = 1$. Assume that $v > 1$. We consider the powers $(ca)^j$ for $j = 0, 1, ...$ If $j \equiv 0 \bmod v$ then $(ca)^j = a^j$ and if $j \equiv 0 \bmod m$ then $(ca)^j = c^j$. Suppose that $(ca)^s = 1$. Then $c^s = a^{-s}$. Lemma 16 above implies that the order of c^s divides m and v thus since m and v are relatively prime we see that $c^s = 1$ and $a^{-s} = 1$. Hence, $c^s = a^s = 1$. Hence $s \equiv 0 \bmod v$ and $s \equiv 0 \bmod m$. This implies that $(mv)|s$. Hence if $v > 1$ then $s > m$. This contradicts the definition of m. Thus $v = 1$. Hence $k = r$. So $k|m$. Write $m = wk$. Then the order of $d = a^w$ is k. Applying Theorem 12 the powers $1, d, d^2, ..., d^{k-1}$ are exactly the roots of the polynomial $t^k - 1$. This says that the roots of $t^k - 1$ form a subset of $\{1, a, a^2, ..., a^{m-1}\}$. But $c^k = 1$ so it is a root of $t^k - 1$. This contradicts the existence of $c \notin \{1, a, a^2, ..., a^{m-1}\}$ and hence $\{1, a, a^2, ..., a^{m-1}\} = F_p - \{0\}$. We conclude that $m = p - 1$. This completes the proof. ■

Definition 18 *An element of order $p-1$ is called a primitive element of F_p (in Rose this is called a primitive root).*

We will now show how this result implies Euler's theorem on quadratic residues. We recall that the Legendre symbol is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } p \nmid a \text{ and } a \text{ is a quadratic residue modulo } p \\ 0 \text{ if } p|a \\ -1 \text{if } p \nmid a \text{ and } a \text{ is not a quadratic residue modulo } p \end{cases}.$$

Theorem 19 *Assume that p is an odd prime. Let $a \in \mathbb{Z}$.*

1. If the congruence class of a is a primitive element of F_p then $\left(\frac{a}{p}\right) = -1$.

2. $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$.

Proof. Let $b \in \mathbb{Z}$ be such that its congruence class, $\zeta \in F_p$, is primitive. Suppose that $\left(\frac{b}{p}\right) = 1$. Then $\zeta = \nu^2$ for some $\nu \in F_p$. Thus $\zeta^{\frac{p-1}{2}} = (\nu^2)^{\frac{p-1}{2}} = \nu^{p-1} = 1$. But every element of $F_p - \{0\}$ is a power of ζ. Thus if $\mu \in F_p - \{0\}$

then $\mu^{\frac{p-1}{2}} = 1$. But then the polynomial $t^{\frac{p-1}{2}} - 1$ has $p-1 > \frac{p-1}{2}$ roots. This contradicts Theorem 12. We have proved 1.

Before we prove 2. we will prove that an element μ in F_p is the square of an element in $F_p - \{0\}$ if and only if $\mu = \zeta^{2j}$ with j an integer. If $\mu = \zeta^{2j}$. Then $\mu = (\zeta^j)^2$ so it is a square. If $\zeta^{2j+1} = \nu^2$ for some $\nu \in F_p$ then $\zeta = \lambda^2$ with $\lambda = \nu/\zeta^j$. This contradicts the first of this theorem. We have thus proved our assertion.

We are now ready to prove 2. If $a \equiv 0 \bmod p$ then $a^{\frac{p-1}{2}} \equiv 0 \bmod p$, if a is a quadratic residue modulo p then the class of a is of the form ζ^{2j} and $(\zeta^{2j})^{\frac{p-1}{2}} = 1$. If a is not a quadratic residue then the class of a is of the form ζ^{2j+1} and $(\zeta^{2j+1})^{\frac{p-1}{2}} = (\zeta^{2j})^{\frac{p-1}{2}}\zeta^{\frac{p-1}{2}} = \zeta^{\frac{p-1}{2}}$. Now $(\zeta^{\frac{p-1}{2}})^2 = 1$ and the two roots of x^2-1 are 1 and $-1 = p-1$. Since $\zeta^{\frac{p-1}{2}} \neq 1$ we must have $\zeta^{\frac{p-1}{2}} = -1$. This completes the proof. ■

We will now give another application of Theorem 17.

Theorem 20 *(Wilson's Theorem) Let $m \in \mathbb{Z}$, $m > 1$. Then m is a prime if and only if $(m-1)! \equiv -1 \bmod m$.*

Proof. Assume that $(m-1)! \equiv -1 \bmod m$. If $1 \leq a < m$ then $c = -\frac{(m-1)!}{a} \in \mathbb{Z}$. We have

$$ca = -(m-1)! \equiv 1 \bmod m.$$

This implies that $\gcd(a, m) = 1$ for all a satisfying $1 \leq a < m$. Hence m is prime.

Suppose that m is a prime. If $m = 2$ then $(m-1)! = 1$ and $1 \equiv -1 \bmod 2$. We may thus assume that m is odd. Then there exists $1 < a < m$ its congruence class a primitive element (root) of F_p. Thus the congruence classes of $1, a, a^2, ..., a^{m-2}$ give a permutation of $1, 2, ..., m-1$. This implies that

$$1 \cdot a \cdot a^2 \cdots a^{m-2} \equiv (m-1)! \bmod m.$$

This implies that

$$a \cdot a^2 \cdots a^{m-2} = a^{1+2+...+(m-2)} = a^{\frac{(m-1)(m-2)}{2}} = (a^{\frac{m-1}{2}})^{m-2}.$$

Thus

$$(m-1)! \equiv (a^{\frac{m-1}{2}})^{m-2} \bmod m.$$

We note that $m-2$ is odd and so Theorem 19 implies the result. ■

Exercises.

1. Let R be a ring. If $f(t) \in R[t]$ we define a function $\overline{f} : R \to R$ by $\overline{f}(r) = f(r)$ for $r \in R$.

a) Show that if $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ then $\overline{f}$ determines f (that is, knowing $\overline{f}$ allows one to compute the coefficients of $f(t)$).

b) If p is a prime and $R = F_p$ then $\overline{f}$ does not determine $f(t)$. (Hint: How many functions are there from F_p to F_p?)

2. Prove that the element b in F-6 is unique.

3. Prove the distributive law for $R[t]$.

4. Let F be a field. Write an algorithm for the computation of $\gcd(f(t), g(t))$ using the division algorithm.

5. Calculate $\gcd(2 + 17t + 24t^2 + 10t^3 + t^4, 1 + t + t^2 + t^3 + t^4)$ in $\mathbb{Q}[t]$. Reduce the coefficients of the polynomials modulo 5 and calculate the GCD in F_5.

6. Let F be a field with a finite number of elements, m. Show that if $a \in F$, $a \neq 0$ then a has finite order and its order divides $m - 1$.

7. Let F be as in 6. Prove that there exists an element $a \neq 0$ in F of order $m - 1$.

8. For which of the fields F_p, $p = 3, 5, 7, 11, 13$ is 2 a primitive element?

9. Show that $t^2 + 1$ has no roots in $\mathbb{Q}$. Show that $t^2 + 1$ has a root in F_p for p a prime such that $p \equiv 1 \bmod 4$.

10. If F is a finite field with exactly n elements then if we add 1 to itself n times we have $1 + 1 + ... + 1 = 0$. (Hint. The elements $1, 1 + 1, 1 + 1 + 1, ...$ can't all be distinct.)

In the next problems we will prove determine the structure of a field with exactly 4 elements. We will assume that F is such a field (we will in the course of the exercises show that it exists).

11. Assume that F is a field with exactly 4 elements. Show that of $x \in F$ then $x + x = 0$. (Hint: Show that $(1 + 1)^2 = 1 + 1 + 1 + 1$ and use Exercise 10.)

12. Show that there exists $\zeta \in F$ with $\zeta^3 = 1$ such that $F = \{0, 1, \zeta, \zeta^2\}$.

13. Let ζ be as in exercise 2. Show that $1 + \zeta = \zeta^2, 1 + \zeta^2 = \zeta$ and $\zeta + \zeta^2 = 1$. (Hint. Prove that $1 + \zeta + \zeta^2 = 0$ by multiplying the expression by $(1 - \zeta)$ and don't forget that $x = -x$ in F.)

14. Writing F as in exercise 12. write out the addition and multiplication tables. Check that these satisfy R-1,2,3,4,5 and F-6. Thus a field with 4 elements exists.