**Correction:** Runtime for Quadratic Sieve

$n = \#$ to factor

$\log n =$ bitlength of $n$

$$\approx O\left(e^{\sqrt[3]{\log n}}\right)$$

approx.

$O(n) = O(e^{\log n}) =$ exp.

$O(\log n) =$ poly

$\mathbb{Z}$ w/ $+, \times$

$-1, 0, 1, 2, 3, \ldots$

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

$\mathbb{F}_p[X]$ w/ $+, \times$

polynomials with coefficients mod p.

$0, 1, 2, \ldots, p-1,$

$X, X+1, X+2, \ldots, X+(p-1),$

$2X, 2X+1, 2X+2, \ldots$

$\vdots$

$(p-1)X, (p-1)X+1, \ldots$

$X^2, X^2+1, \ldots$

$X^2+X, X^2+X+1, \ldots$

$a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0$

$a_i \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}.$

## $\mathbb{Z}$

operations $+, \times$

Ex $1+3=4$

$3\cdot 7 = 21$

## $\mathbb{F}_p[x]$

operations $+, \times$

Ex. In $\mathbb{F}_2[x]$:

$$x^2 + (x+1) = x^2+x+1$$

$$x + x = 2x = 0$$

$$(x+1)^2 = x^2+2x+1 = x^2+1$$

$$-1 = 1$$

In $\mathbb{F}_7[x]$:

$$(x+1)^2 = x^2+2x+1$$

## Division Algorithm

Given $a, b \in \mathbb{Z}$, $\exists\, q, r \in \mathbb{Z}$

s.t. $a = b \cdot q + r$,

$0 \le r < |b|$.

$$
\begin{array}{rl}
 & \;\;\;\;\;\;73 \leftarrow \text{quotient } q \\
b \rightarrow 3 & \overline{)\,220} \leftarrow a \\
 & \;\;\underline{21\;\;} \\
 & \;\;\;\;10 \\
 & \;\;\;\;\;\underline{\;9} \\
 & \;\;\;\;\;\;1 \leftarrow \text{Remainder } r
\end{array}
$$

## Division Algorithm

Given $a(x), b(x) \in \mathbb{F}_p[x]$,

$\exists\, q(x), r(x) \in \mathbb{F}_p[x]$

s.t. $a(x) = b(x)q(x) + r(x)$,

$0 \le \deg r(x) < \deg b(x)$.

In $\mathbb{F}_2[x]$

$$
\begin{array}{rl}
 & \qquad\quad\;\; x + 1 \\
x^2+1 & \overline{)\,x^3 + x^2 + 0 \cdot x + 1} \\
 & \;\underline{x^3 \qquad\;\; + x \qquad} \\
 & \qquad\; x^2 + x + 1 \\
 & \qquad\; \underline{x^2 \qquad\;\; + 1} \\
 & \qquad\qquad\; x
\end{array}
$$

$(x^2+1)(x+1) + x$

$= x^3 + x^2 + \cancel{x} + 1 + \cancel{x}$

$= x^3 + x^2 + 1$ ✓

# (Extended) Euclidean Alg.

$\gcd(16, 6)$

$$16 = 2 \cdot 6 + 4$$

$$6 = 1 \cdot 4 + 2 \leftarrow \gcd$$

$$4 = 2 \cdot 2 + 0$$

$$\boxed{16x + 6y = 2}$$

$$\boxed{\begin{array}{c}16\\ x=1\\ y=0\end{array}} = 2 \cdot \boxed{\begin{array}{c}6\\ x=0\\ y=1\end{array}} + \boxed{\begin{array}{c}4\\ x=1\\ y=-2\end{array}}$$

$$\boxed{\begin{array}{c}6\\ x=0\\ y=1\end{array}} = 1 \cdot \boxed{\begin{array}{c}4\\ x=1\\ y=-2\end{array}} + \boxed{\begin{array}{c}2\\ x=-1\\ y=3\end{array}} \leftarrow \text{done}$$

# (Extended) Euclidean Alg.

$\gcd(x^3+x^2+x+1,\ x^3+1)$ in $\mathbb{F}_2[x]$

$$x^3+x^2+x+1 = 1 \cdot (x^3+1) + x^2+x$$

$$x^3+1 = (x+1)(x^2+x) + (x+1) \leftarrow \gcd$$

$$x^3 + \cancel{x^2} + \cancel{x^2} + x$$

$$x^2+x = x \cdot (x+1) + 0$$

$$\underline{s}(x^3+x^2+x+1) + \underline{t}(x^3+1) = x+1$$

$$\boxed{\begin{array}{c}x^3+x^2+x+1\\ s=1\\ t=0\end{array}} = 1 \cdot \boxed{\begin{array}{c}x^3+1\\ s=0\\ t=1\end{array}} + \boxed{\begin{array}{c}x^2+x\\ s=1\\ t=1\end{array}}$$

$-1 = 1 \bmod 2$

$$\boxed{\begin{array}{c}x^3+1\\ s=0\\ t=1\end{array}} = (x+1)\boxed{\begin{array}{c}x^2+x\\ s=1\\ t=1\end{array}} + \boxed{\begin{array}{c}x+1\\ s=x+1\\ t=x\end{array}}$$

$2 = 0 \bmod 2$

$$\Rightarrow (x+1)(x^3+x^2+x+1) + x(x^3+1) \overset{\checkmark}{=} x+1$$

| $\mathbb{Z}$ | $\mathbb{F}_p[x]$ |
| --- | --- |
| <u>Def<sup></sup>n</u>. Let $m \in \mathbb{Z}$. Then $a \equiv b \pmod m$ if $m \mid a-b$. | <u>Def<sup></sup>n</u> Let $m(x) \in \mathbb{F}_p[x]$. Two polynomials $a(x), b(x) \in \mathbb{F}_p[x]$ satisfy $a(x) \equiv b(x) \bmod m(x)$ if $m(x) \mid a(x) - b(x)$. |
| <u>Def<sup></sup>n</u>. $\mathbb{Z}/m\mathbb{Z}$ is the set of equivalence classes mod $m$. | <u>Def<sup></sup>n</u>. $\mathbb{F}_p[x]/(m(x))$ is the set of equivalence classes mod $m(x)$. |
| <u>Ex.</u> $3 \cdot 2 \equiv 6 \equiv 1 \pmod 5$<br>$3 + 3 \equiv 6 \equiv 1 \pmod 5$ | <u>Ex.</u> In $\mathbb{F}_3[x]$,<br>$\times x^3$<br>$(x^2+1)(x^2+x) \equiv x^4 + x^3 + x^2 + x \equiv 0 \pmod{x+1}$<br>$x^2 + x + 1 \equiv 2^2 + 2 + 1 \equiv 1 \pmod{x+1}$<br>$x+1 \equiv 0$<br>$x \equiv -1$<br>$x \equiv 2$ |

## $\mathbb{Z}$

**Thm.** If $a \equiv b \pmod{m}$
$c \equiv d \pmod{m}$

Then $a + c \equiv b + d \pmod{m}$
$ac \equiv bd \pmod{m}$

**Prop** ① If $0 \le r_1, r_2 < m$
then $\underset{(\text{mod } m)}{r_1 \equiv r_2} \Rightarrow r_1 = r_2$.

② If $r \ge m$
then $\underset{(\text{mod } m)}{r \equiv r'}$ w/ $0 \le r' < m$.

**Therefore:** $\mathbb{Z}/m\mathbb{Z} = \{0, 1, \ldots, m-1\}$

$|\mathbb{Z}/m\mathbb{Z}| = m$.

## $\mathbb{F}_p[x]$

**Thm.** If $a(x) \equiv b(x) \pmod{m(x)}$
$c(x) \equiv d(x) \pmod{m(x)}$

Then $a(x) + c(x) \equiv b(x) + d(x)$
$a(x)c(x) \equiv b(x)d(x)$
$\pmod{m(x)}$

**Prop** ① If $r_1(x), r_2(x)$ have $\deg < \deg m(x)$
then $\underset{(\text{mod } m(x))}{r_1(x) \equiv r_2(x)} \Rightarrow r_1(x) = r_2(x)$.

② If $\deg r(x) \ge \deg m(x)$
then $r(x) \equiv r_1(x)$ w/ $\deg r_1(x) < \deg m(x)$.

So $\mathbb{F}_p[x]/(m(x)) = \{ r(x) : \deg r < \deg m \}$

If $d = \deg m$ $\quad = \{ a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 : a_i \in \mathbb{F}_p \}$

( $d$ coefficients, $p$ options for each )

$|\mathbb{F}_p[x]/(m(x))| = p^d$.

**Example.** $\mathbb{F}_2[x]/(x^2+x+1) = \{0, 1, x, x+1\}$

Modular Arithm. **Rule 1**: $2=0$, $-1=1$

Eg. $x+x = 2x = 0\cdot x = 0$

**Rule 2**: $x^2+x+1=0$

$x^2 = -x-1$

$x^2 = x+1$

| + | 0 | 1 | x | x+1 |
|---|---|---|---|---|
| 0 | 0 | 1 | x | x+1 |
| 1 | 1 | 0 | x+1 | x |
| x | x | x+1 | 0 | 1 |
| x+1 | x+1 | x | 1 | 0 |

| × | 0 | 1 | x | x+1 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | x | x+1 |
| x | 0 | x | x+1 | 1 |
| x+1 | 0 | x+1 | 1 | x |

Eg. $x\cdot x = x^2 = x+1$

$$\begin{aligned} x(x+1) &= x^2+x \\ &= (x+1)+x \\ &= 2x+1 \\ &= 0\cdot x+1 \\ &= 1 \end{aligned}$$

$$\begin{aligned} (x+1)(x+1) &= x^2+2x+1 \\ &= x^2+1 \\ &= x+1+1 \\ &= x \end{aligned}$$

Q: What is the multiplicative inverse of $x+1$?

A: $x$ (from the table).

Q: Which elements are invertible and which are not?

Yes: all except 0.

No: 0

This called the $\boxed{\text{finite field of 4 elements.}}$ Denoted $\mathbb{F}_4$. $\neq \mathbb{Z}/4\mathbb{Z}$ ✱

**Def$^n$** A *field* is a set $F$ w/ $+, \cdot : F \times F \longrightarrow F$, s.t.

0) $0, 1 \in F$ where
   $0$ is additive identity: $0 + a = a + 0 = a \quad \forall\, a \in F$.
   $1$ is mult. identity: $1 \cdot a = a \cdot 1 = a \quad \forall\, a \in F$.

1) $+, \cdot$ are associative and commutative
   $(x \cdot y) \cdot z = x \cdot (y \cdot z) \qquad x \cdot y = y \cdot x$.

2) $\cdot$ distributes over $+$ : $z(x+y) = z \cdot x + z \cdot y$

3) a) everything has an additive inverse: $\forall\, a \in F,\ \exists\, -a \in F,\ a + (-a) = 0$.
   b) everything non-zero has a multiplicative inverse: $\forall\, a \in F,\ \exists\, a^{-1} \in F,\ a \cdot a^{-1} = 1$.

**Examples:** $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ when $p$ is prime.
$\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$.

Note: A *ring* is a field except for 3b) fails

**Non-Examples:** $\mathbb{Z}/n\mathbb{Z}$ when $n$ is composite.

# Finite Fields in General

**Fact:** If $m(x)$ is irreducible $\overbrace{\text{over } \mathbb{F}_p}^{\text{in } \mathbb{F}_p[x]}$,

then $\mathbb{F}_p[x] / (m(x))$ is a field of size $p^{\deg m}$.

It has elements $\{ a_0 + a_1 x + \dots + a_{d-1} x^{d-1} : a_i \in \mathbb{F}_p,\ d = \deg m \}$

**Def$^n$.** A polynomial $m(x) \in \mathbb{F}_p[x]$ is irreducible if it cannot be expressed as a product of lower degree polynomials.

Ex. In $\mathbb{F}_2[x]$, $x^2+1 = (x+1)(x+1)$ is not irreducible

but $x^2+x+1$ is.

(Analog to "composite".)

Notation: $\mathbb{F}_{p^d}$ or $GF(p^d)$ where $d = \deg m$.

**Fact:** Finite fields are isomorphic iff they have the same size.

**Fact:** There exists $\mathbb{F}_{p^d}$ $\forall$ $p$ prime and $d \geq 1$.