Correction: Runtime for Quadratic Sieve

n = # to factor

$\log n$ = bitlength of n

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

↑ approx.

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

$O(\log n) = \text{poly}$

$\mathbb{Z}$ 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.

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

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

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

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

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

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

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

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

$\mathbb{Z}$

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

$0 \le r < |b|$.

$$
\begin{array}{r|l}
 & 73 \leftarrow \text{quotient } q \\
\hline
3 & 220 \leftarrow a \\
 & 21\downarrow \\
\hline
 & 10 \\
 & 9 \\
\hline
 & 1 \leftarrow \text{Remainder } r
\end{array}
$$

$b \uparrow$

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 $\mathbb{F}_2[x]$

$$
\begin{array}{r|l}
 & x+1 \\
\hline
x^2+1 & x^3 + x^2 + 0\cdot x + 1 \\
 & x^3 \quad + x \quad \downarrow \\
\hline
 & x^2 + x + 1 \\
 & x^2 \quad\quad + 1 \\
\hline
 & x
\end{array}
$$

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

$= x^3 + x^2 + x + 1 + x$

$= x^3 + x^2 + 1$ ✓

Division Algorithm

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

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

$0 \le r < |b|$.

$$
\begin{array}{r|l}
 & 73 \leftarrow \text{quotient } q \\
\hline
3 & 220 \leftarrow a \\
 & 21\downarrow \\
\hline
 & 10 \\
 & 9 \\
\hline
 & 1 \leftarrow \text{Remainder } r
\end{array}
$$

$b \uparrow$

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 $\mathbb{F}_2[x]$

$$
\begin{array}{r|l}
 & x+1 \\
\hline
x^2+1 & x^3 + x^2 + 0\cdot x + 1 \\
 & x^3 \quad + x \quad \downarrow \\
\hline
 & x^2 + x + 1 \\
 & x^2 \quad\quad + 1 \\
\hline
 & x
\end{array}
$$

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

$= x^3 + x^2 + x + 1 + x$

$= x^3 + x^2 + 1$ ✓

(Extended) Euclidean Alg.

$\gcd(16, 6)$

$16 = 2 \cdot 6 + 4$

$6 = 1 \cdot 4 + \boxed{2} \leftarrow \gcd$

$4 = 2 \cdot 2 + 0$

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

16 $x=1$ $y=0$	$= 2 \cdot$	6 $x=0$ $y=1$	$+$	4 $x=1$ $y=-2$		
6 $x=0$ $y=1$	$= 1 \cdot$	4 $x=1$ $y=-2$	$+$	2 $x=-1$ $y=3$	← done	

(Extended) Euclidean Alg.

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

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

$x^3+1 = (x+1)(x^2+x) + (x+1)$ ← gcd

$x^3+x^2+x^2+x$

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

$s(x^3+x^2+x+1) + t(x^3+1) = x+1$

x^3+x^2+x+1 $s=1$ $t=0$	$= 1 \cdot$	x^3+1 $s=0$ $t=1$	$+$	x^2+x $s=1$ $t=1$	$-1 = 1 \bmod 2$	
x^3+1 $s=0$ $t=1$	$= (x+1) \cdot$	x^2+x $s=1$ $t=1$	$+$	$x+1$ $s=x+1$ $t=x$	$2 = 0 \bmod 2$	

$\Rightarrow (x+1)(x^3+x^2+x+1) + x(x^3+1) = x+1$ ✓

$\mathbb{Z}$

Def^n. Let $m \in \mathbb{Z}$.
Then $a \equiv b \pmod{m}$ if
$m \mid a-b$.

Def^n. $\mathbb{Z}/m\mathbb{Z}$ is the set of equivalence classes mod m.

Ex. $3 \cdot 2 \equiv 6 \equiv 1 \pmod 5$

$3+3 \equiv 6 \equiv 1 \pmod 5$

$\mathbb{F}_p[x]$

Def^n Let $m(x) \in \mathbb{F}_p[x]$.
Two polynomials $a(x), b(x) \in \mathbb{F}_p[x]$
satisfy $a(x) \equiv b(x) \mod m(x)$
if $m(x) \mid a(x) - b(x)$.

Def^n. $\mathbb{F}_p[x]/(m(x))$ is the set of equivalence classes mod $m(x)$.

Ex. In $\mathbb{F}_3[x]$,

$(x^2+1)(x^2+x) \equiv x^4 + x^3 + x^2 + x$ (mod $x+1$)
$\equiv 0$

$x \cdot x^3$

$x^2 + x + 1 \equiv 2^2 + 2 + 1$ (mod $x+1$)
$\equiv 1$

$x+1 \equiv 0$
$x \equiv -1$
$x \equiv 2$