

Notes on Arithmetic of Some Commutative Rings and Fields

October 1993

G.R. Blakley

## INDEX

1. MODULAR ARITHMETIC	11
2. CASTING OUT NINES, TENS AND ELEVENS	21
3. MULTIPLE PRECISION ARITHMETIC	31
4. THE BINARY METHOD OF RAISING A BASE TO A POWER	41
5. A FIRST CUT AT NUMBER THEORY: PRIMES, COMPOSITES, $\varphi, \lambda$ FERMAT'S, EULER'S AND CARMICHAEL'S THEOREMS	51
6. THE EUCLIDEAN ALGORITHM FOR INTEGERS	61
7. THE ARITHMETIC OF POLYNOMIALS	71
8. THE EUCLIDEAN ALGORITHM FOR POLYNOMIALS. FIRST CUT	81
9. THE ARITHMETIC OF POLYNOMIALS WHOSE COEFFICIENT ARITHMETIC IS MODULO 2 ARITHMETIC	91
10. THE EUCLIDEAN ALGORITHM FOR POLYNOMIALS. SECOND CUT	101
11. FINDING RECIPROCAL MODULO $m$	111
12. A SECOND CUT AT NUMBER THEORY: THE DISTRIBUTION OF PRIMES	121
13. REDUCIBILITY AND IRREDUCIBILITY	131
14. FIELDS. ESPECIALLY GALOIS FIELDS	141
15. SMART DISPLAYS OF TABLES FOR SMALL GALOIS FIELDS	151
16. GALOIS FIELDS.	161

## 1. MODULAR ARITHMETIC.

9 hours after 8 PM isn't 17 PM. It's 5 AM. This is an example of modulo 12 arithmetic.  $9 + 8 = 17 = 12 + 5$ . So we write  $9 + 8 \equiv 5 \pmod{12}$ .

**Definition 11.** More generally  $a \equiv b \pmod{m}$  means that  $b - a$  is a multiple of  $m$ . Equivalently,  $a \equiv b \pmod{m}$  means that  $b$  and  $a$  leave the same remainder upon division by  $m$ . The expression  $a \equiv b \pmod{m}$  is sometimes abbreviated  $a \equiv_m b$ .

**Lemma 11. Congruence** modulo a positive integer  $m$  has three properties.

REFLEXIVE.  $\forall a,$   $a \equiv a \pmod{m}$

SYMMETRIC.  $\forall a, \forall b,$   $a \equiv b \pmod{m}$  if  $b \equiv a \pmod{m}$

TRANSITIVE.  $\forall a, \forall b, \forall c,$   $a \equiv c \pmod{m}$  if both  $a \equiv b \pmod{m}$  and  $b \equiv c \pmod{m}$ .

**Lemma 12.** Congruence is an **equivalence relation**. Its **blocks (equivalence classes)** form a **partition** of the set

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$$

of **integers**.

**Example 11.** The five blocks modulo 5 are

$$\text{BLOCK}(-2) = \text{BLOCK}(18) = \dots = \{\dots, -12, -7, -2, 3, 8, 13, 18, \dots\}$$

$$\text{BLOCK}(4) = \text{BLOCK}(9) = \dots = \{\dots, -11, -6, -1, 4, 9, 14, 19, \dots\}$$

$$\text{BLOCK}(0) = \text{BLOCK}(15) = \dots = \{\dots, -10, -5, 0, 5, 10, 15, 20, \dots\}$$

$$\text{BLOCK}(-9) = \text{BLOCK}(-4) = \dots = \{\dots, -9, -4, 1, 6, 11, 16, 21, \dots\}$$

$$\text{BLOCK}(-8) = \text{BLOCK}(17) = \dots = \{\dots, -8, -3, 2, 7, 12, 17, 22, \dots\}$$

The blocks of a partition  $\pi$  of a set  $S$  are always like this. In other words:

**Lemma 13.** No block is the empty set  $\emptyset$ .

If  $\pi$  and  $\psi$  are blocks and  $\pi \cap \psi \neq \emptyset$ , then  $\pi = \psi$ .

$S$  is the union of all the blocks of  $\pi$ .

**Lemma 14.** If  $a \equiv \alpha \pmod{m}$  and  $b \equiv \beta \pmod{m}$ , then

$$a + b \equiv \alpha + \beta \pmod{m}$$

$$a - b \equiv \alpha - \beta \pmod{m}$$

$$a * b \equiv \alpha * \beta \pmod{m}.$$

**Example 12.** Thus

$$\begin{aligned} 101 &= 96 + 5 = (8)12 + 5 \equiv 5 \\ -2425 &= -2436 + 11 = (-203)12 + 11 \equiv 11. \end{aligned}$$

**Example 13.** And, predictably,

$$(101)(-2425) = -244925 = -244932 + 7 = (-20411)12 + 7 \equiv 7$$

in agreement with

$$(5)(11) = 55 = 48 + 7 = (4)12 + 7 \equiv 7.$$

**Example 14.** Also

$$101 + (-2425) = -2324 = -2328 + 4 = (-194)12 + 4 \equiv 4$$

in agreement with

$$5 + 11 = 16 = 12 + 4 = (1)12 + 4 \equiv 4.$$

**Example 15.** Finally

$$101 - (-2425) = 2526 = 2520 + 6 = (210)12 + 6 \equiv 6$$

in agreement with

$$5 - 11 = -6 = 12 + 6 = (1)12 + 6 \equiv 6.$$

## 2. CASTING OUT NINES, TENS AND ELEVENES.

People were once taught to check work by casting out nines, and by casting out elevens.

Here goes.

**Example 21.** Consider casting out nines.

$$(1696\ 6375)_9 + 6 = 1\ 5269\ 7375 + 6 = 1\ 5269\ 7381 \equiv_9 1+5+2+6+9+7+3+8+1 = 42 \equiv_9 4+2 = 6.$$

This is **not** a coincidence. If you add up the digits of a number  $n$ , the sum of these digits is congruent to  $n$  modulo 9. (Why?) This is the basis for casting out nines.

**Example 22.** Now consider casting out elevens.

$$\begin{aligned}(1388\ 1580)_{11} + 2 &= 1\ 5269\ 7380 + 2 = 1\ 5269\ 7382 \equiv_{11} (1 + 2 + 9 + 3 + 2) - (5 + 6 + 7 + 8) \\ &= 17 - 26 = -9 \equiv_{11} 2.\end{aligned}$$

**Example 23.** Also

$$\begin{aligned}(1\ 6436\ 9165)_{11} + 10 &= 18\ 0806\ 0815 + 10 = 18\ 0806\ 0825 \equiv_{11} \\ &\equiv_{11} (8 + 8 + 6 + 8 + 5) - (1 + 0 + 0 + 0 + 2) = 35 - 3 = 32 \equiv_{11} 2 - 3 = -1 \equiv_{11} 10\end{aligned}$$

These **aren't** coincidences. Start with a number  $q$ . Add up its alternate digits starting from the last (rightmost, least significant, “ones man”) to get  $a$ . Then add up alternate digits of  $q$  starting from the penultimate (next-to-rightmost, next-to-least-significant, “tens man”) to get  $s$ . Form  $a - s$ .

**Lemma 21.** This difference,  $a - s$ , is congruent to  $q$  modulo 11.

(Why?) Well, that’s how to cast out nines and cast out elevens.

Congruence respects sums, differences and products. (Lemma 14, reworded.) So there are cheap checks.

**Example 24.** Is  $123 * 456 = 5\ 6088$ ?

	nines	elevens
123	6	2
*456	*6	*5
<u>5 6088</u>	<u>0</u>	<u>10</u>
	checks	checks

Probably  $123 * 456 = 5\ 6088$ , since it passes both checks.

**Example 25.** Is  $123 * 456 = 5\ 0688$ ?

	nines	elevens
123	6	2
*456	*6	*5
<u>5 0688</u>	<u>0</u>	<u>0</u>
	checks	no check

Certainly  $123 * 456 \neq 5\ 0688$ , since it fails the casting-out-elevens check

**Example 26.** Is  $123 * 456 = 5\ 6077$ ?

	nines	elevens
123	6	2
*456	*6	*5
<u>5 6077</u>	<u>7</u>	<u>10</u>
	no check	checks

Certainly  $123 * 456 \neq 5\ 6077$ , since it fails the casting-out-nines check.

**Example 27.** Is  $123 * 456 = 5\ 6078$ ?

	nines	elevens
123	6	2
*456	*6	*5
<u>5 6078</u>	<u>8</u>	<u>0</u>
	no check	no check

Very **very** certainly  $123 * 456 \neq 5\ 6078$ , since it fails **both** the casting-out-nines check **and** the casting-out-elevens check.

**Example 28.** Is  $123 * 456 = 2327\ 8221$ ?

	nines	elevens
123	6	2
*456	*6	*5
2327 8221	0	10
—————	—————	—————
	checks	checks

Probably  $123 * 456 = 2327\ 8221$ , since it passes both checks.

To summarize:

probably	$123 * 456 = 5\ 6088$
certainly	$123 * 456 \neq 5\ 0688$
certainly	$123 * 456 \neq 5\ 6077$
very very certainly	$123 * 456 \neq 5\ 6078$
probably	$123 * 456 = 2327\ 8821$ .

Not bad. There are two opinions not worth countenancing, and one **very** abhorrent opinion. On the other hand, there are two plausible alternatives. So

**Conundrum 21.** Should people of good will keep an open mind as to whether

$$123 * 456 = 5\ 6088$$

or

$$123 * 456 = 2327\ 8821$$

or neither? Any comments?

By the way, casting-out-nines checks and casting-out-elevens checks work as well on addition and subtraction as they do on multiplication. Just how well is that?

You've been casting-out-tens during most of your school years. If somebody claims that

$$123456789 * 987654321 = 128$$

you instantly **know** that he's wrong! Why? Because  $9 * 1 \neq 8$ . Work with last digits (*i.e.* rightmost digits, least significant digits, ones men).

Last digit of sum = last digit of sum of last digits.

Last digit of product = last digit of product of last digits.

Last digit of difference = WELL, WHAT?

It's now obvious how to cast out twos (*i.e.* to appeal to the arithmetic of EVEN and ODD) and how to cast out fives.

What about casting out sevens? Thirteens.

In **octal arithmetic** (where nine is written 11 and ten is written 12) how do you cast out sevens? How do you cast out nines? Twos? Fours? Fives? Elevens?

### 3. MULTIPLE PRECISION ARITHMETIC.

Consider a 2-digit computer which uses two windows (registers) to display the up-to-four digits resulting from an integer multiply. If it is tasked to perform the multiplication

$$12\ 3456 * 98\ 7654$$

it might use a triple-precision calculation along the following lines. It can make use of obvious facts, such as

$$\begin{array}{r} 12\ 0000 \\ 3400 \\ 56 \\ \hline 12\ 3456 \end{array} \qquad \begin{array}{r} 98\ 0000 \\ 7600 \\ 54 \\ \hline 98\ 7654 \end{array}$$

This suggests a multiplication table within the capabilities of this pitiful computer. See Figure 31 below.

Collecting the results shown in Figure 31 below, our poor weak two-digit computer assembles its partial results

$$\begin{array}{r} 1176\ 0000\ 0000 \\ 42\ 4400\ 0000 \\ 8720\ 0000 \\ 60\ 9200 \\ 3024 \\ \hline \end{array}$$

It then adds-with-carry in two-digit-window gulps to get

$$\begin{array}{r} 1\ 1\ 1\ 8\ 3\ 1\ 8\ 0\ 2\ 2\ 2\ 4 \\ 1\ 1\ 0\ 1\ 0 \end{array}$$

Then the carries ripple once

$$1219\ 3181\ 2224$$

In this case there is no need for further carry ripples. In other cases there could be more. Our feeble two-digit computer has thus formed the twelve-digit product of two six-digit strings (*i.e.* two three-feeble-computer-word strings). Using this triple precision arithmetic approach you can find a thirty-digit product of two fifteen-digit integers on a calculator whose ten-digit window can show the full product of two five-digit numbers.

Let's cast out nines

$$\begin{array}{rcllcl}
 12 & 3456 & \rightarrow & 1 + 2 + 3 + 4 + 5 + 6 & \rightarrow & 21 & \longrightarrow & 3 \\
 98 & 7654 & \rightarrow & 9 + 8 + 7 + 6 + 5 + 4 & \rightarrow & 39 & \rightarrow 12 \rightarrow & 3 \\
 \\ 
 1219 & 3181 & 2224 & \rightarrow & 1 + 2 + 1 + 9 + 3 + 1 + 8 + 1 + 2 + 2 + 2 + 4 & \rightarrow & 36 & \rightarrow 9 \rightarrow & 0
 \end{array}$$

It checks. Now tens.

$$\begin{array}{rcl}
 12 & 3456 & \longrightarrow 6 \\
 98 & 7654 & \longrightarrow 4 \\
 \\ 
 1219 & 3181 & 2224 & \longrightarrow 4
 \end{array}$$

It checks. Now elevens.

$$\begin{array}{rcllcl}
 12 & 3456 & \rightarrow & (6 + 4 + 2) - (5 + 3 + 1) & \rightarrow & 3 \\
 98 & 7654 & \rightarrow & (4 + 6 + 8) - (5 + 7 + 9) & \rightarrow & -3 & \rightarrow & 8 \\
 \\ 
 1219 & 3181 & 2224 & \rightarrow & (4 + 2 + 1 + 1 + 9 + 2) - (2 + 2 + 8 + 3 + 1 + 1) & \rightarrow & 2
 \end{array}$$

It checks. So, in a sense, we are more than 99.8% confident that the product is correct.

Now go and invent multiple precision arithmetic in general.

Lots of people think a 1024-bit RSA is a pretty strong cryptosystem in 1993. There are CRAYS with 256-bit words.

So you ought to have a fourfold-precision arithmetic routine at your disposal for such RSA computations on such a CRAY.

If you have to rely on a 16-bit processor, then it might be advisable to have sixty-four-fold precision arithmetic at your disposal for RSA encrypt/decrypt work on that processor.

#### 4. THE BINARY METHOD OF RAISING A BASE TO A POWER

Consider forming the **power**

$$a \equiv 37^{6243} \pmod{6\,5537}$$

It looks as if it requires 6242 multiplications modulo 6 5537. But you can actually get by with 17 multiplications modulo 6 5537 as follows

$$\begin{array}{rcl}
 37^2 & \equiv & 1369 \\
 37^4 & \equiv & 1369^2 \equiv 3\,9125 \\
 37^8 & \equiv & 3\,9125^2 \equiv 1\,7916 \\
 37^{16} & \equiv & 1\,7916^2 \equiv 4\,8367 \\
 37^{32} & \equiv & 4\,8367^2 \equiv 2\,3474 \\
 37^{64} & \equiv & 2\,3474^2 \equiv 5\,9117 \\
 37^{128} & \equiv & 5\,9117^2 \equiv 5\,9164 \\
 37^{256} & \equiv & 5\,9164^2 \equiv 4\,7726 \\
 37^{512} & \equiv & 4\,7726^2 \equiv 3\,2641 \\
 37^{1024} & \equiv & 3\,2641^2 \equiv 6\,5409 \\
 37^{2048} & \equiv & 6\,5409^2 \equiv 1\,6384 \\
 37^{4096} & \equiv & 1\,6384^2 \equiv 6\,1441 \\
 37^3 & \equiv & 37^{2+1} \equiv 1369 * 37 \equiv 5\,0653 \\
 37^{35} & \equiv & 37^{32+2+1} \equiv 2\,3474 * 5\,0653 \equiv 5\,6268 \\
 37^{99} & \equiv & 37^{64+32+2+1} \equiv 5\,9117 * 5\,6268 \equiv 6\,4921 \\
 37^{2147} & \equiv & 37^{2048+64+32+2+1} \equiv 1\,6384 * 6\,4921 \equiv 154 \\
 37^{6243} & \equiv & 37^{4096+2048+64+32+2+1} \equiv 6\,1441 * 154 \equiv 2\,4586
 \end{array}$$

This is the **binary method** (Knuth, vol. 2) of raising a **base** to a **power**. The number of multiplications required is obviously no more than twice the **log** (base two) of the **exponent**. So you can raise a base  $b$  to a 200-digit exponent with fewer than 1400 modular multiplies. NEVER NEVER NEVER NEVER NEVER (Shakespeare, Lear, V, iii) do real arithmetic on a calculator or a computer when you have integer arithmetic to do.

NEVER NEVER NEVER NEVER NEVER (Churchill, Fulton, Missouri, speech) use  $**$  in Fortran, or  $\uparrow$  in Algol, or  $y^x$  on a calculator, when you are taking powers in modular arithmetic.

**Do integer multiplies, and use exact multiple precision integer arithmetic,** when you are calculating powers modulo  $m$ .

5. A FIRST CUT AT NUMBER THEORY: PRIMES, COMPOSITES,  $\varphi$ ,  $\lambda$ , FERMAT'S, EULER'S, AND CARMICHAEL'S THEOREMS.

**Definition 51.** A **prime** is an integer  $p \geq 2$  with no factors belonging to the set  $\{2, 3, 4, \dots, p-2, p-1\}$ . An integer  $c \geq 2$  is **composite** if  $c$  is not prime, *i.e.* if there are integers  $a$  and  $b$  belonging to the set  $\{2, 3, 4, \dots, p-2, p-1\}$  such that  $ab = c$ .

**Definition 52.** A prime  $p$  is a **Fermat prime** if there is a nonnegative integer  $N$  such that

$$p = 1 + 2^{2^N}.$$

The **Fermat number**  $F(N)$  is  $F(N) = 1 + 2^{2^N}$ . Thus  $\log(F(N) - 1) = 2^N$ , *i.e.*

$$\log(\log(F(N) - 1)) = N.$$

The Fermat primes known widely in the summer of 1993 are

$$F(0) = 1 + 2^{2^0} = 1 + 2^1 = 3$$

$$F(1) = 1 + 2^{2^1} = 1 + 2^2 = 1 + 4 = 5$$

$$F(2) = 1 + 2^{2^2} = 1 + 2^4 = 1 + 16 = 17$$

$$F(3) = 1 + 2^{2^3} = 1 + 2^8 = 1 + 256 = 257$$

$$F(4) = 1 + 2^{2^4} = 1 + 2^{16} = 1 + 65536 = 65537$$

The Fermat numbers  $F(5)$ ,  $F(6)$ ,  $F(7)$ ,  $F(8)$  and  $F(9)$  have been fully factored.  $F(N)$  is composite if  $5 \leq N \leq 21$ . In summer 1993 it was not known whether  $F(22)$  is prime. Some people think  $F(4)$  is the largest Fermat prime.

**Definition 53.** A prime  $p$  is a **Mersenne prime** if there is a prime  $q$  such that

$$p = -1 + 2^q.$$

The **Mersenne number**  $M(q)$  is  $M(q) = -1 + 2^q$ . Thus  $\log(M(q) + 1) = q$ .

The 32 Mersenne primes known widely in the summer of 1993 are

$$M(2) = -1 + 2^2 = -1 + 4 = 3$$

$$M(3) = -1 + 2^3 = -1 + 8 = 7$$

$$M(5) = -1 + 2^5 = -1 + 32 = 31$$

$$M(7) = -1 + 2^7 = -1 + 128 = 128$$

$$M(13) = -1 + 2^{13} = -1 + 8192 = 8191$$

$$M(17) = -1 + 2^{17} = -1 + 131072 = 131071$$

$$M(19) = -1 + 2^{19} = -1 + 524288 = 524287$$

$$M(31) = -1 + 2^{31} = 2147483647$$

$$M(61) = -1 + 2^{61}$$

$$M(89) = -1 + 2^{89}$$

$$M(107) = -1 + 2^{107}$$

$$M(127) = -1 + 2^{127}$$

$$M(521) = -1 + 2^{521}$$

$$M(607) = -1 + 2^{607}$$

$$M(1279) = -1 + 2^{1279}$$

$$M(2203)$$

$$M(2281)$$

$$M(3217)$$

$$M(4253)$$

$$M(4423)$$

$M(9689)$   
 $M(9941)$   
 $M(1\ 1213)$   
 $M(1\ 9937)$   
 $M(2\ 1701)$   
  
 $M(2\ 3209)$   
 $M(4\ 4497)$   
 $M(8\ 6243)$   
 $M(11\ 0503)$   
 $M(13\ 2049)$   
  
 $M(21\ 6091)$   
 $\vdots$   
 $M(75\ 6839),$

a 22 7832-digit number.

There are no other Mersenne primes less than  $M(21\ 6091)$ . There may be other Mersenne primes between  $M(21\ 6091)$  and  $M(75\ 6839)$ . Most of the time, the largest known prime is a Mersenne prime. Many people think there are infinitely many Mersenne primes.

**Example 51.** Note that

$$\begin{array}{rclclcl}
 0^{7-1} & = & 0^6 & = & 0 & = & 0 & + & 0 * 7 & \equiv & 0 \pmod{7} \\
 1^{7-1} & = & 1^6 & = & 1 & = & 1 & + & 1 * 7 & \equiv & 1 \pmod{7} \\
 2^{7-1} & = & 2^6 & = & 64 & = & 1 & + & 9 * 7 & \equiv & 1 \pmod{7} \\
 3^{7-1} & = & 3^6 & = & 729 & = & 1 & + & 104 * 7 & \equiv & 1 \pmod{7} \\
 4^{7-1} & = & 4^6 & = & 4096 & = & 1 & + & 585 * 7 & \equiv & 1 \pmod{7} \\
 5^{7-1} & = & 5^6 & = & 1\ 5625 & = & 1 & + & 2232 * 7 & \equiv & 1 \pmod{7} \\
 6^{7-1} & = & 6^6 & = & 4\ 6656 & = & 1 & + & 6665 * 7 & \equiv & 1 \pmod{7}
 \end{array}$$

And that's the way it is with **prime** moduli.

**Fermat's Theorem 52.** Suppose that  $m$  is a prime. Suppose that  $a$  is not congruent to zero modulo  $m$ . Then  $a^{m-1} \equiv 1 \pmod{m}$ .

With composite moduli, it's slightly more complicated.

**Definition 54.** Euler's **totient function**  $\varphi$  is defined as follows. Let  $a$  be a positive integer.

$$\begin{aligned}\varphi(p^a) &= (p-1)p^{a-1} && \text{if } p \text{ is prime} \\ \varphi(a * b) &= \varphi(a) * \varphi(b) && \text{if } \gcd(a, b) = 1.\end{aligned}$$

**Fact 51.**  $\varphi(m)$  counts how many numbers  $x$  in the  $m$ -member set

$$S(m) = \{0, 1, 2, \dots, m-2, m-1\}$$

satisfy the condition  $\gcd(x, m) = 1$ .

**Definition 55.** Carmichael's **universal exponent function**  $\lambda$  is defined as follows.

$$\begin{aligned}\lambda(1) &= \lambda(2) = \lambda(4) = 1 \\ \lambda(2^{a+1}) &= 2^{a-1} && \text{if } a \text{ is an integer larger than } 1 \\ \lambda(p^a) &= (p-1)p^{a-1} && \text{if } p \text{ is an odd prime} \\ \lambda(a * b) &= \ell cm(a, b) && \text{if } \gcd(a, b) = 1\end{aligned}$$

**Fact 52.**  $\lambda(m)$  is the smallest positive integer exponent such that  $a^{\lambda(m)} \equiv 1 \pmod{m}$  for every  $a$  such that  $\gcd(a, m) = 1$ .

**Fact 53.**  $\varphi(m)$  is a positive integer multiple of  $\lambda(m)$  for every positive integer  $m$ .

Consider some examples.

**Example 52.**  $\varphi(5) = 5 - 1 = 4$ , and

$$\gcd(1, 5) = \gcd(2, 5) = \gcd(3, 5) = \gcd(4, 5) = 1.$$

But  $\gcd(0, 5) = 5$ .

Also  $\lambda(5) = 4$ , since  $1^4 \equiv 2^4 \equiv 3^4 \equiv 4^4 \equiv 1 \pmod{5}$ , but  $2^1 \equiv 2 \pmod{5}$ ,  $2^2 \equiv 4 \pmod{5}$ ,  $2^3 \equiv 3 \pmod{5}$ .

**Example 53.**

$$\begin{aligned}\varphi(180) &= \varphi(2^2 3^2 5^1) \\ &= \varphi(2^2)\varphi(3^2)\varphi(5^1) \\ &= (2-1)2^{2-1}(3-1)3^{2-1}(5-1)5^{1-1} \\ &= 1 * 2 * 2 * 3 * 4 * 1 \\ &= 48 \\ \lambda(180) &= \lambda(2^2 3^2 5^1) \\ &= \text{lcm}(\lambda(2^2), \lambda(3^2), \lambda(5^1)) \\ &= \text{lcm}(1, 6, 4) \\ &= 12.\end{aligned}$$

It is easy to verify that  $\gcd(x, 180) = 1$  for each of the 48 numbers  $x$  belonging to the set  $\{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 77, 79, 83, 89, 91, 97, 101, 103, 107, 109, 113, 119, 121, 127, 131, 133, 137, 139, 143, 149, 151, 157, 161, 163, 167, 169, 173, 179\}$  of integers relatively prime to  $m$ .

It is also easy to verify that  $2 \leq \gcd(y, 180)$  for each of the 132 numbers  $y$  belonging to the set  $\{0, 2, 3, 4, 5, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30, 32, 33, 34, 35, 36, 38, 39, 40, 42, 44, \dots, 174, 175, 176, 177, 178\}$  of integers which are not relatively prime to  $m$ .

The fundamental theorem of arithmetic says that a positive integer can be factorized into primes in a manner which is unique up to order.

**Theorem 53.** Let  $m$  be an integer strictly larger than 1. Let  $a = (a(1), a(2), \dots, a(s))$  and  $b = (b(1), b(2), \dots, b(t))$  be lists of primes. Suppose that

$$a(1) * a(2) * \dots * a(s) = b(1) * b(2) * \dots * b(t) = m.$$

Then  $s = t$ , and there is a member of  $\psi$  of  $SYM(\{1, 2, \dots, s\})$  (*i.e.* a permutation  $\psi$  of the set  $\{1, 2, \dots, s\}$  underlying the lists  $a$  and  $b$ ), such that

$$\begin{aligned} a(1) &= b(\psi(1)) \\ a(2) &= b(\psi(2)) \\ &\vdots \\ a(s) &= b(\psi(s)). \end{aligned}$$

**Example 54.** The following lists

$$\begin{aligned} a &= (2, 3, 7, 11, 2, 3, 7, 3) \\ b &= (2, 3, 7, 11, 3, 7, 2, 3) \\ c &= (2, 2, 3, 3, 3, 7, 7, 11) \end{aligned}$$

are rearrangements of one another. Every entry on each list is prime. Therefore the three product representations

$$\begin{aligned} 2 * 3 * 7 * 11 * 2 * 3 * 7 * 3 &= 5\ 8212 \\ 2 * 3 * 7 * 11 * 3 * 7 * 2 * 3 &= 5\ 8212 \\ 2 * 2 * 3 * 3 * 3 * 7 * 7 * 11 &= 5\ 8212 \end{aligned}$$

are three of the many **fundamental theorem of arithmetic decompositions** (*ftads*) of 5 8212.

**Example 55.** Neither of the product representations

$$\begin{aligned} 1 * 2 * 2 * 3 * 3 * 3 * 7 * 7 * 11 &= 5\ 8212 \\ 6 * 6 * 3 * 7 * 7 * 11 &= 5\ 8212 \end{aligned}$$

is an *ftad* of 5 8212.

**Comments 51.** Because of the associative and commutative laws, the unordered power product  $\prod_{a \in A} a^{e(a)}$  makes sense (*i.e.* is **well defined**) for any nonvoid finite set  $A$  of integers and any function  $e$  from  $A$  to the set of positive integers. Obviously the *fta* is equivalent to the statement that every integer  $m$  has a unique representation

$$m = \prod_{p \in A} p^{e(p)}$$

where  $A$  is a finite set of primes and  $e(p)$  is the multiplicity of  $p$ . For example, the unordered power product *ftad* of 5 8212 is given by

$$A = \{2, 3, 7, 11\}$$

$$e(2) = 2$$

$$e(3) = 3$$

$$e(7) = 2$$

$$e(11) = 1$$

$$\prod_{p \in A} p^{e(p)} = 2^2 * 3^3 * 7^2 * 11^1 = 7^2 * 3^3 * 2^2 * 11^1 = 5\ 8212.$$

The unordered power product representation on the left of the last line above is unique. It happens to equal each of the (nonunique) ordered power product representations in the middle of that line.

**Example 56.**

$$\begin{aligned}\varphi(5\ 8212) &= \varphi(4 * 27 * 49 * 11) \\ &= \varphi(2^2 * 3^3 * 7^2 * 11^1) \\ &= \varphi(2^2)\varphi(3^3)\varphi(7^2)\varphi(11) \\ &= (2 - 1)2^{2-1}(3 - 1)3^{3-1}(7 - 1)7^{2-1}(11 - 1)11^{1-1} \\ &= 1 * 2 * 2 * 9 * 6 * 7 * 10 \\ &= 1\ 5120 \\ &= 24 * 630 \\ \lambda(5\ 8212) &= \lambda(2^2 * 3^3 * 7^2 * 11^1) \\ &= lcm(\lambda(2^2), \lambda(3^3), \lambda(7^2), \lambda(11)) \\ &= lcm(1, (3 - 1)3^{3-1}, (7 - 1)7^{2-1}, (11 - 1)11^{1-1}) \\ &= lcm(1, 2 * 9, 6 * 7, 10) \\ &= lcm(1, 18, 42, 10) \\ &= 630\end{aligned}$$

Table 51 below records values of  $\varphi$  and of  $\lambda$ . It is easy to verify.

**Euler's Theorem 54.** Suppose that  $gcd(a, m) = 1$ . Then  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

**Carmichael's Theorem 55.** Suppose that  $gcd(a, m) = 1$ . Then  $a^{\lambda(m)} \equiv 1 \pmod{m}$ . If  $1 \leq t \leq \lambda(m) - 1$ , then there is an integer  $b$  such that  $gcd(b, m) = 1$  and  $b^t \not\equiv 1 \pmod{m}$ .

**Related Theorem 56.** Suppose that  $gcd(a, m) \neq 1$ . Then no positive integer power of  $a$  is congruent to 1 modulo  $m$ .

---

$m$	1	2	3	4	5	6	7	8	9	10	11	12	13
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10	4	12
$\lambda(m)$	1	1	2	1	4	2	6	2	6	4	10	2	12

$m$	14	15	16	17	18	19	20	21	22	23	24	25
$\varphi(m)$	6	8	8	16	12	18	8	12	10	22	8	20
$\lambda(m)$	6	4	4	16	12	18	4	6	10	22	2	20

$m$	26	27	28	29	30	31	32	33	34	35	36	37
$\varphi(m)$	12	18	12	28	8	30	16	20	16	24	12	36
$\lambda(m)$	12	18	6	28	4	30	8	10	8	12	6	36

$m$	38	39	40	41	42	43	44	45	46	47	48	49
$\varphi(m)$	18	24	16	40	12	42	20	24	22	46	16	42
$\lambda(m)$	18	12	4	41	6	42	10	12	22	46	4	42

**Table 51**

---

## 6. THE EUCLIDEAN ALGORITHM FOR INTEGERS.

The **euclidean algorithm** is an ancient recipe which produces the greatest common divisor,  $gcd(u, v)$ , of two integers,  $u$  and  $v$ , and writes it as an **integer linear combination** of them.

$$gcd(u, v) = su + tv \quad (s \text{ and } t \text{ are integers})$$

The Aho/Hopcroft/Ullman [The Design and Analysis of Computer Algorithms, Addison-Wesley, Reading, Massachusetts (1974)] version of the euclidean algorithm uses matrix-theoretic row operations to find  $gcd$ s. For example, the  $gcd$  of 8 2530 7441 and 1255 5221 is

### Example 61.

remainder	quotient	copies of 8 2430 7441	copies of 1255 5221
8 2530 7441		1	-0
1255 5221	= 65 + ...	-0	1
921 8076	= 1 + ...	1	-65
333 7145	= 2 + ...	-1	66
254 3786	= 1 + ...	3	-197
79 3359	= 3 + ...	-4	263
16 3709	= 4 + ...	15	-986
13 8523	= 1 + ...	-64	4207
2 5186	= 5 + ...	79	-5193
1 2593	= 2 exactly	-459	3 0172
0	is undefined	997	-6 5537

Thus, using multiple precision arithmetic, we verify that

$$\begin{aligned}
 gcd(8\ 2530\ 7441, 1255\ 5221) &= 1\ 2593 = -378\ 81611\ 5419 + 3788\ 1612\ 8012 \\
 &= (-459)(8\ 2530\ 7441) + (3\ 0172)(1255\ 5221)
 \end{aligned}$$

**Note 61.** The congruences

$$1255\ 5221x = 1 \pmod{8\ 2530\ 7441}$$

$$\text{and } 8\ 2530\ 7441x = 1 \pmod{1255\ 5221}$$

are therefore unsolvable! Also

$$\begin{array}{rclcl} 1\ 2593 & * & 997 & = & 1255\ 5221 \\ 1\ 2593 & * & 6\ 5537 & = & 8\ 2530\ 7441 \end{array}$$

If you factored to get the *gcd*, you would try the first 55 primes

2,	3,	5,	7	11,	13,	17,	19,	23,	29,
31,	37,	41,	43,	47,	53,	59,	61,	67,	71,
73,	79,	83,	89,	97,	101,	103,	107,	109,	113,
127,	131,	137,	139,	149,	151,	157,	163,	167,	173,
179,	181,	191,	193,	197,	199,	211,	223,	227,	229,
233,	239,	241,	251,	257					

as possible divisors of 8 2530 7441 and of 1255 5221 to get the fundamental theorem of arithmetic decompositions (ftads)

$$\begin{array}{rclcl} 8\ 2530\ 7441 & = & 1\ 1790\ 1063 * 7 & = & 1684\ 3009 * 7 * 7 \\ & = & 6\ 5537 * 257 * 7 * 7 & = & 6\ 5537 * 1\ 2593 \\ \\ 1255\ 5221 & = & 179\ 3603 * 7 & = & 25\ 6229 * 7 * 7 \\ & = & 997 * 257 * 7 * 7 & = & 997 * 1\ 2593 \end{array}$$

**Fact 61.** Since  $257 * 257 = 6\ 6049 > 6\ 5537 > 997$ , you know that both 6 5537 and 997 are primes.

So the job of finding the value, 1 2593, of the *gcd* is done. But this (55 + 55)-step process would take more time to carry out than the construction of the 11-row euclidean algorithm table above.

You can take the *gcd* of any two 11-digit numbers by means of a euclidean algorithm table with fewer than 55 row operations. But if you throw the fundamental theorem of arithmetic at the problem, you might wind up trying all primes less than 31 6228 as possible divisors of each of the two numbers. There are more than 2 7000 such primes.

**Moral 61.** Factoring is **not** a good way (indeed, in this course, not an acceptable way) to find a greatest common divisor. **Stick to the euclidean algorithm.**

A natural question arises. We have found one way to write

$$1\,2593 = 8\,2530\,7441\,s + 1255\,5221\,t$$

as a linear combination of  $8\,2530\,7441$  and  $1255\,5221$  using integer weights  $s$  and  $t$ . What are all others pairs  $(s, t)$  of weights? Obviously they all lie on a line. But how widely are they spaced, and where are they?

**Fact 62.** The only integer pairs  $(s, t)$  such that

$$1\,2593 = 8\,2530\,7441\,s + 1255\,5221\,t$$

are of the form

$$(s, t) = (-459 + 997w, 3\,0172 - 6\,5537w)$$

where  $w$  is any integer.

The last (*i.e.* bottom) two rows of the Aho/Hopcroft/Ullman approach to  $gcd$  extraction thus give a complete answer to the question of representing  $gcd(u, v) = us + vt$  in all possible ways as an integer linear combination of  $u$  and  $v$ .

This Aho/Hopcroft/Ullman approach (using matrices and row operations) **is the only one which will be accepted** in this course. And the answer to a  $gcd(u, v)$  extraction problem will **always** involve an **explicit** formula for **all** integer linear representations  $gcd(u, v) = us + vt$ .

**Theorem 61.** The Euclidean algorithm for  $gcd(u, v)$  takes no more than  $1.5 \log(u)$  row operations [Knuth, vol. 2 p. 357]. Thus the complete table has less than  $3 \log(u)$  rows.

**Theorem 52.** The worst case of the Euclidean algorithm occurs when  $u$  and  $v$  are successive Fibonacci numbers.

See [Knuth, vol. 2, p. 343] for the exact statement of Theorem 62.

A shorter example is

**Example 62.**

remainders	quotients	copies of 119	copies of 84
119		1	-0
	1+		
84		-0	1
	2+		
35		1	-1
	2+		
14		-2	3
	2 exactly		
7		5	-7
	is undefined		
0		-12	17

From the penultimate line we see

$$\gcd(119, 84) = 7 = 595 - 588 = 119(5) + 84(-7)$$

From the ultimate line we extend this to the more informative statement that the representatives

$$\gcd(119, 84) = [595 - 1428t] - [588 - 1428t] = 119[5 - 12t] + 84[-7 + 17t]$$

(for any integer  $t$ ) are the only representations of  $\gcd(119, 84)$  as an integer linear combination  $119x + 84y$  of 119 and 84. These integer points are located at intervals of  $\sqrt{433}$  along a line of slope  $-17/12$  on the points  $(5, -7)$  and  $(-7, 10)$  in the  $(a, b)$  plane. Clearly

$$\gcd(119, 84) = 7 = 119(-7) + 84(10) = 119(5) + 84(-7)$$

and the distance between  $(5, -7)$  and  $(-7, 10)$  is  $\sqrt{433}$ .

Our upper bound of 9 row operations for the eleven-row table in Example 62 is pessimistic. So is our upper bound of 35 to the actual 21 rows in the table in Example 61.

**Problem 61.** Work out the Euclidean algorithm for the first two Fibonacci numbers larger than 200. How pessimistic are our bounds?

## 7. THE ARITHMETIC OF POLYNOMIALS.

The euclidean algorithm also works on polynomials. Consider

$$p(x) = x^4 + 2x^3 - 2x^2 - 14x - 35 = (1, 2, -2, -14, -35)$$

$$u(x) = x^5 - 6x^3 + 3x^2 - 7x - 21 = (1, 0, -6, 3, -7, -21).$$

**Example 71.** To add  $p(x) + u(x)$

$$\begin{array}{r} \phantom{+} \phantom{1} \phantom{0} \phantom{-6} \phantom{3} \phantom{-7} \phantom{-21} \\ + \phantom{1} \phantom{0} \phantom{-6} \phantom{3} \phantom{-7} \phantom{-21} \\ \hline 1 \phantom{0} \phantom{-6} \phantom{3} \phantom{-7} \phantom{-21} \phantom{-56} \\ \phantom{1} 1 \phantom{-6} \phantom{3} \phantom{-7} \phantom{-21} \phantom{-56} \\ \phantom{1} \phantom{1} -4 \phantom{3} \phantom{-7} \phantom{-21} \phantom{-56} \\ \phantom{1} \phantom{1} \phantom{-4} 1 \phantom{-7} \phantom{-21} \phantom{-56} \\ \phantom{1} \phantom{1} \phantom{-4} \phantom{1} -21 \phantom{-56} \\ \phantom{1} \phantom{1} \phantom{-4} \phantom{1} \phantom{-21} -56 \end{array}$$

Therefore

$$p(x) + u(x) = x^5 + x^4 - 4x^3 + x^2 - 21x - 56 = (1, 1, -4, 1, -21, -56)$$

Subtraction is so similar that there is no need to show it here.

**Example 72.** To multiply  $p(x) * u(x)$ , use a multiplication table

		1	2	-2	-14	-35	*
1	2	-2	-14	-35			1
	0	0	0	0	0		0
		-6	-12	12	84	210	-6
			3	6	-6	-42	3
				-7	-14	14	-7
					-21	-42	-21
1	2	-8	-23	-24	43	140	35
							539
							735

The above process is called the Cauchy multiplication of polynomials (and extends to power series and even Laurent series). At any rate we see that

$$\begin{aligned} p(x) * u(x) &= x^9 + 2x^8 - 8x^7 - 23x^6 - 24x^5 + 43x^4 + 140x^3 + 35x^2 + 539x + 735 \\ &= (1, 2, -8, -23, -24, 43, 140, 35, 539, 735) \end{aligned}$$



## 8. THE EUCLIDEAN ALGORITHM FOR POLYNOMIALS. FIRST CUT.

**Assertion 81:** The greatest common divisor of the  $p(x)$  and  $u(x)$  of Section 7 is

$$13x^2 - 91 = (1)(x^5 - 6x^3 + 3x^2 - 7x - 21) \\ + (-x + 2)(x^4 + 2x^3 - 2x^2 - 14x - 35)$$

Of course, there's no harm in saying that the  $gcd$  in question is  $x^2 - 7$ , or is  $(1/7)x^2 - 1$ , or is  $130x^2 - 910$ , or is  $(1/28)x^2 - 1/4$ .

The form of the  $gcd$  many people prefer is the rather simple looking monic polynomial (*i.e.*, polynomial whose leading coefficient is equal to 1)

$$x^2 - 7 = (1/13)(x^5 - 6x^3 + 3x^2 - 7x - 21) \\ + (1/13)(-x + 2)(x^4 + 2x^3 - 2x^2 - 14x - 35)$$

**Assertion 82:** Also, the last line of Example 75 says that

$$0 = (1/13)(-x^2 - 2x - 5)(x^5 - 6x^3 + 3x^2 - 7x - 21) \\ + (1/13)(x^3 + x + 3)(x^4 + 2x^3 - 2x^2 - 14x - 35)$$

Let's check these assertions. The only nontrivial multiplication in Example 75 is

1	2	-2	-14	-35		*	
-1	-2	2	14	35		-1	
	2	4	-4	-28	-70		2
-1	0	6	10	7	-70		

The addition then is

1	0	-6	3	-7	-21
-1	0	6	10	7	-70
			13	0	-91

Therefore Assertion 81 is true. The multiplications in Assertion 82 are (forgetting the common factor of  $1/13$ )

$$\begin{array}{cccccc|c}
 & 1 & 2 & -2 & -14 & -35 & | & * \\
 \hline
 1 & 2 & -2 & -14 & -35 & & | & 1 \\
 & 0 & 0 & 0 & 0 & 0 & | & 0 \\
 & & 1 & 2 & -2 & -14 & -35 & | & 1 \\
 & & & 3 & 6 & -6 & -42 & -105 & | & 3 \\
 \hline
 \end{array}$$

$$\begin{array}{cccccccc}
 1 & 2 & -1 & -9 & -31 & -21 & -77 & -105
 \end{array}$$

and

$$\begin{array}{cccccc|c}
 & 1 & 0 & -6 & 3 & -7 & -21 & | & * \\
 \hline
 -1 & 0 & 6 & -3 & 7 & 21 & & | & -1 \\
 & -2 & 0 & 12 & -6 & 14 & 42 & | & -2 \\
 & & -5 & 0 & 30 & -15 & 35 & 105 & | & -5 \\
 \hline
 -1 & -2 & 1 & 9 & 31 & 20 & 77 & 105
 \end{array}$$

So the sum is, indeed,

$$\begin{array}{cccccccc}
 1 & 2 & -1 & -9 & -31 & -20 & -77 & -105 \\
 -1 & -2 & 1 & 9 & 31 & 20 & 77 & 105 \\
 \hline
 & & & & & & & 0
 \end{array}$$

What if we had tried to find the *gcd* by factorization? It would have been a daunting task. However, now that we know the *gcd*, we can do long division of  $x^2 - 7$  into  $p(x)$  and  $u(x)$ .



9. THE ARITHMETIC OF POLYNOMIALS WHOSE COEFFICIENT ARITHMETIC IS MODULO 2 ARITHMETIC.

We will now redo these examples in the arithmetic of the integers modulo 2. Thus

$$-6 \equiv_{\frac{2}{2}} -14 \equiv_{\frac{2}{2}} 2 \equiv_{\frac{2}{2}} 0.$$

Also  $21 \equiv_{\frac{2}{2}} 13 \equiv_{\frac{2}{2}} -7 \equiv_{\frac{2}{2}} 1$ . Moreover,  $x + y \equiv_{\frac{2}{2}} x - y$  (George Orwell's law), and so on. This time

$$p(x) = x^4 + 1 = (1, 0, 0, 0, 1) = 1\ 0001$$

$$u(x) = x^5 + x^2 + x + 1 = (1, 0, 0, 1, 1, 1) = 10\ 0111$$

**Example 91.** Their sum is

$$\begin{array}{r} 1\ 0001 \\ +10\ 0111 \\ \hline \end{array}$$

$$11\ 0110 = x^5 + x^4 + x^2 + x$$

**Example 92.** Their difference also is

$$\begin{array}{r} 1\ 0001 \\ -10\ 0111 \\ \hline \end{array}$$

$$11\ 0110 = x^5 + x^4 + x^2 + x$$

(Remember the Orwellian rule modulo two: PLUS IS MINUS).

**Example 93.** Their product is

$$\begin{array}{r|l} 1\ 0001 & * \\ \hline 10\ 001 & 1 \\ 0\ 0000 & 0 \\ 0000\ 0 & 0 \\ 100\ 01 & 1 \end{array}$$

$$\begin{array}{r|l} 10\ 001 & 1 \\ 1\ 0001 & 1 \\ \hline \end{array}$$

$$10\ 0101\ 0111 = x^9 + x^6 + x^4 + x^2 + x + 1$$

**Example 94.** The long division is

$$\begin{array}{r}
 10 \\
 10001 \overline{) 100111} \\
 \underline{10001} \\
 101
 \end{array}
 = \text{quotient} = q(x) = x$$

$$= \text{remainder} = r(x) = x^2 + 1$$

**Example 95.** The next division is

$$\begin{array}{r}
 101 \\
 101 \overline{) 10001} \\
 \underline{101} \\
 10 \\
 \underline{0} \\
 101 \\
 \underline{101} \\
 0
 \end{array}
 = \text{quotient} = v(x) = x^2 + 1$$

$$= \text{remainder} = w(x) = 0$$

## 10. THE EUCLIDEAN ALGORITHM FOR POLYNOMIALS. SECOND CUT.

**Example 101.** The euclidean algorithm is

remainders	quotients	copies of $u(x)$	copies of $p(x)$
10 0111		1	0
<hr/>	= 10 with remainder		
1 0001		0	1
<hr/>	= 101 exactly		
101		1	10
<hr/>	is undefined		
0		101	1011

Thus the  $gcd$  of  $p(x)$  and  $u(x)$  is  $101 = (1, 0, 1) = x^2 + 1$ . It can't avoid being monic. Also, it's unique! Why? Because the only nonzero number you can multiply it by is 1.

As in Section 8 above, somebody who has calculated this  $gcd$  can long divide 101 into 1 0001 and into 10 0111 to get the following factorizations.

$$x^4 + 1 = 1\ 0001 = 101 * 101 = (x^2 + 1) * (x^2 + 1)$$

$$x^5 + x^2 + x + 1 = 10\ 0111 = 101 * 1011 = (x^2 + 1) * (x^3 + x + 1)$$

**Example 102.** Then we can go further, and notice that  $101 = 11 * 11$ , but that 1011 is irreducible in coefficient arithmetic modulo two. You cannot factor

$$1011 = x^3 + x + 1$$

nontrivially into two lower degree polynomials using modulo 2 arithmetic on its coefficients.

**Example 103.** You can factor  $x^3 + x + 1$  as the product of a linear polynomial and a quadratic polynomial (I don't know what they are, though I could find out. How?) in real arithmetic.

**Example 104.** You can even split it (factor it into the product of three linear polynomials) in complex arithmetic.

**Example 105.** Also, most importantly, you can split it

$$x^3 + x + 1 = (x + 2)(x + 4)(x + 6) = (x - 2)(x - 4)(x - 6)$$

if you use  $GF(8)$  arithmetic on its coefficients.  $GF(8)$  arithmetic will be explained in Section 14 below. The reader is warned here that the arabic symbols 2, 4, 6 above are **not** the two, four, six of grammar school arithmetic. See Sections 13, 14 and 15 below.

Well, what about comparing our five different versions of the  $gcd$  in high-school arithmetic?

	high school arithmetic	:	modulo two arithmetic
$(13, 0, -91) =$	$13x^2 - 91$	:	$x^2 + 1 = 101$
$(1, 0, 7) =$	$x^2 - 7$	:	$x^2 + 1 = 101$
$(1/7, 0, -1) =$	$(1/7)x^2 - 1$	:	$(1/1)x^2 + 1 = 101$
$(130, 0, -910) =$	$130x^2 - 910$	:	$0x^2 + 0 = 0$
$(1/28, 0, -1/4) =$	$(1/28)x^2 - 1/4$	:	$(1/0)x^2 + 1/0 = ?$

The first three high-school forms of the  $gcd$  work like a charm in the arithmetic of the integers modulo 2.

The fourth high-school form is zero times the true  $gcd$  modulo 2. And we won't accept that, any more than we would accept  $0 * 1\ 2593 = 0$  as a  $gcd$  of  $8\ 2530\ 7441$  and  $1255\ 5221$  when we are working with integers. The only integers which are  $gcds$  of these two numbers are  $-1\ 2593$  and  $1\ 2593$ .

The fifth high-school form is worse still modulo 2. It amounts to  $(1/0)(x^2 + 1)$ . And that is a nonsense expression. There's no more use trying to divide by a **disguised** zero than by an **undisguised** zero. And, if you are doing arithmetic modulo two, the symbols  $1/28$  and  $-1/4$  are merely disguises for good old  $1/0$ , the *I-don't-know* symbol.

From these considerations we draw a working principle.

**Principle 101.** If you are doing coefficient arithmetic modulo a prime  $p$  concurrently with polynomial arithmetic modulo an irreducible polynomial  $\pi(x)$  you can avoid some kinds of grief by reducing mod  $p$  before and during reduction mod  $\pi(x)$ , rather than after reduction mod  $\pi(x)$ .

Well, it's pretty obvious that the modulo two arithmetic of polynomials is a lot easier than the high school arithmetic of the very same polynomials. We'll use it from here on out.

A lot of people hate long bit strings. So, after doing the dirty work above, they abbreviate it all in octal ("digits" allowed are 0, 1, 2, 3, 4, 5, 6, 7) or hexadecimal ("digits" allowed are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F) notation. This is much easier to read and makes the work look prettier. It also makes the worker look like an absolute genius, since hex or octal do not come naturally to most people. Indeed, the most brazen of them omit to mention the binary background and leave the impression that it's easier for them to work directly in octal or hex. The fact of the matter is that you could learn to work directly in octal or hex with no more trouble than it takes a school child to learn ordinary arithmetic.

At any rate, here is a Rosetta Stone [see Kahn, *Codebreakers*, 901-912] with three ways of summarizing the polynomial arithmetic.

BINARY	OCTAL	HEXADECIMAL																																																																
$\begin{array}{r} 1\ 0001 \\ + 10\ 0111 \\ \hline 11\ 0110 \end{array}$	$\begin{array}{r} 21 \\ + 47 \\ \hline 66 \end{array}$	$\begin{array}{r} 11 \\ + 27 \\ \hline 36 \end{array}$																																																																
$\begin{array}{r} 1\ 0001 \\ - 10\ 0111 \\ \hline 11\ 0110 \end{array}$	$\begin{array}{r} 21 \\ - 47 \\ \hline 66 \end{array}$	$\begin{array}{r} 11 \\ - 27 \\ \hline 36 \end{array}$																																																																
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%; text-align: center;">1 0001</td> <td style="width: 5%; text-align: center;"> </td> <td style="width: 5%; text-align: center;">*</td> <td style="width: 55%;"></td> </tr> <tr> <td style="border-top: 1px solid black; text-align: center;">10 001</td> <td style="border-top: 1px solid black; text-align: center;"> </td> <td style="border-top: 1px solid black; text-align: center;">1</td> <td></td> </tr> <tr> <td style="text-align: center;">0 0000</td> <td style="text-align: center;"> </td> <td style="text-align: center;">0</td> <td></td> </tr> <tr> <td style="text-align: center;">0000 0</td> <td style="text-align: center;"> </td> <td style="text-align: center;">0</td> <td></td> </tr> <tr> <td style="text-align: center;">100 01</td> <td style="text-align: center;"> </td> <td style="text-align: center;">1</td> <td></td> </tr> <tr> <td style="text-align: center;">10 001</td> <td style="text-align: center;"> </td> <td style="text-align: center;">1</td> <td></td> </tr> <tr> <td style="text-align: center;">1 0001</td> <td style="text-align: center;"> </td> <td style="text-align: center;">1</td> <td></td> </tr> <tr> <td style="border-top: 1px solid black; text-align: center;">10 0101 0111</td> <td></td> <td></td> <td></td> </tr> </table>	1 0001		*		10 001		1		0 0000		0		0000 0		0		100 01		1		10 001		1		1 0001		1		10 0101 0111				<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%; text-align: center;">21</td> <td style="width: 5%; text-align: center;"> </td> <td style="width: 5%; text-align: center;">*</td> <td style="width: 55%;"></td> </tr> <tr> <td style="border-top: 1px solid black; text-align: center;">104</td> <td style="border-top: 1px solid black; text-align: center;"> </td> <td style="border-top: 1px solid black; text-align: center;">4</td> <td></td> </tr> <tr> <td style="text-align: center;">167</td> <td style="text-align: center;"> </td> <td style="text-align: center;">7</td> <td></td> </tr> <tr> <td style="border-top: 1px solid black; text-align: center;">1127</td> <td></td> <td></td> <td></td> </tr> </table>	21		*		104		4		167		7		1127				<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%; text-align: center;">11</td> <td style="width: 5%; text-align: center;"> </td> <td style="width: 5%; text-align: center;">*</td> <td style="width: 55%;"></td> </tr> <tr> <td style="border-top: 1px solid black; text-align: center;">22</td> <td style="border-top: 1px solid black; text-align: center;"> </td> <td style="border-top: 1px solid black; text-align: center;">2</td> <td></td> </tr> <tr> <td style="text-align: center;">77</td> <td style="text-align: center;"> </td> <td style="text-align: center;">7</td> <td></td> </tr> <tr> <td style="border-top: 1px solid black; text-align: center;">257</td> <td></td> <td></td> <td></td> </tr> </table>	11		*		22		2		77		7		257			
1 0001		*																																																																
10 001		1																																																																
0 0000		0																																																																
0000 0		0																																																																
100 01		1																																																																
10 001		1																																																																
1 0001		1																																																																
10 0101 0111																																																																		
21		*																																																																
104		4																																																																
167		7																																																																
1127																																																																		
11		*																																																																
22		2																																																																
77		7																																																																
257																																																																		
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;"></td> <td style="width: 5%;"></td> <td style="width: 5%; text-align: center;">10</td> <td style="width: 55%;"></td> </tr> <tr> <td style="text-align: center;">1 0001</td> <td style="text-align: center;"> </td> <td style="border-top: 1px solid black; text-align: center;">100 0111</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> </td> <td style="text-align: center;">100 01</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> </td> <td style="border-top: 1px solid black; text-align: center;">101</td> <td></td> </tr> </table>			10		1 0001		100 0111				100 01				101		<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;"></td> <td style="width: 5%;"></td> <td style="width: 5%; text-align: center;">2</td> <td style="width: 55%;"></td> </tr> <tr> <td style="text-align: center;">21</td> <td style="text-align: center;"> </td> <td style="border-top: 1px solid black; text-align: center;">47</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> </td> <td style="text-align: center;">42</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> </td> <td style="border-top: 1px solid black; text-align: center;">5</td> <td></td> </tr> </table>			2		21		47				42				5		<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;"></td> <td style="width: 5%;"></td> <td style="width: 5%; text-align: center;">2</td> <td style="width: 55%;"></td> </tr> <tr> <td style="text-align: center;">11</td> <td style="text-align: center;"> </td> <td style="border-top: 1px solid black; text-align: center;">27</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> </td> <td style="text-align: center;">22</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> </td> <td style="border-top: 1px solid black; text-align: center;">5</td> <td></td> </tr> </table>			2		11		27				22				5																	
		10																																																																
1 0001		100 0111																																																																
		100 01																																																																
		101																																																																
		2																																																																
21		47																																																																
		42																																																																
		5																																																																
		2																																																																
11		27																																																																
		22																																																																
		5																																																																
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;"></td> <td style="width: 5%;"></td> <td style="width: 5%; text-align: center;">5</td> <td style="width: 55%;"></td> </tr> <tr> <td style="text-align: center;">101</td> <td style="text-align: center;"> </td> <td style="border-top: 1px solid black; text-align: center;">1 0001</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> </td> <td style="text-align: center;">1 01</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> </td> <td style="border-top: 1px solid black; text-align: center;">10</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> </td> <td style="text-align: center;">0</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> </td> <td style="border-top: 1px solid black; text-align: center;">101</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> </td> <td style="text-align: center;">101</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> </td> <td style="border-top: 1px solid black; text-align: center;">0</td> <td></td> </tr> </table>			5		101		1 0001				1 01				10				0				101				101				0		<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;"></td> <td style="width: 5%;"></td> <td style="width: 5%; text-align: center;">5</td> <td style="width: 55%;"></td> </tr> <tr> <td style="text-align: center;">5</td> <td style="text-align: center;"> </td> <td style="border-top: 1px solid black; text-align: center;">21</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> </td> <td style="text-align: center;">21</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> </td> <td style="border-top: 1px solid black; text-align: center;">0</td> <td></td> </tr> </table>			5		5		21				21				0		<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;"></td> <td style="width: 5%;"></td> <td style="width: 5%; text-align: center;">5</td> <td style="width: 55%;"></td> </tr> <tr> <td style="text-align: center;">5</td> <td style="text-align: center;"> </td> <td style="border-top: 1px solid black; text-align: center;">11</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> </td> <td style="text-align: center;">11</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"> </td> <td style="border-top: 1px solid black; text-align: center;">0</td> <td></td> </tr> </table>			5		5		11				11				0	
		5																																																																
101		1 0001																																																																
		1 01																																																																
		10																																																																
		0																																																																
		101																																																																
		101																																																																
		0																																																																
		5																																																																
5		21																																																																
		21																																																																
		0																																																																
		5																																																																
5		11																																																																
		11																																																																
		0																																																																

**Figure 101.** The Top Half of the Rosetta Stone for binary, octal and hex.

BINARY

rems	quots	copies of 10 0111	copies of 1 0001
10 0111		1	0
	= 10+		
1 0001		0	1
	= 101 exactly		
105		1	10
	is undefined		
0		101	1011

OCTAL

rems	quots	copies of of 47	copies of of 21
47		1	0
	= 2+		
21		0	1
	= 5 exactly		
5		1	2
	is undefined		
0		5	13

HEXADECIMAL

rems	quots	copies of of 27	copies of of 11
27		1	0
	= 2+		
11		0	1
	= 5 exactly		
5		1	2
	is undefined		
0		5	<i>B</i>

**Figure 102.** The Bottom Half of the Rosetta Stone for binary, octal and hex.

## 11. FINDING RECIPROCAL MODULO $m$ .

It is important to be able to solve a **linear congruence**, *i.e.* a congruence of the form

$$ab \equiv 1 \pmod{m}$$

for  $b$  (given  $a$  and  $m$ ) whether  $a, b$  and  $m$  are integers or whether they are polynomials. Finding  $b$  is finding  $1/a$ , *i.e.* is finding the **reciprocal** of  $a$ . If you can find  $1/a$ , you can then find  $c/a$  by defining

$$c/a := c * (1/a).$$

To solve  $ab = 1 \pmod{m}$ , just throw the Aho/Hopcroft/Ullman version of the Euclidean algorithm at  $a$  and  $m$ .

If  $a$  and  $m$  **are not relatively prime** (*i.e.* if they have a nontrivial common factor), the euclidean algorithm will tell you so. It will produce a  $gcd$  which is not 1 (Actually, it will produce neither 1 nor  $-1$  in the integer case, and it will produce a nonconstant polynomial in the polynomial case.) If either of these things happen, there is no solution  $b$  to the congruence.

If  $a$  and  $m$  **are relatively prime**, it will produce a  $gcd$  which amounts to 1 (1 or  $-1$  in the integer case, a nonzero constant polynomial in the polynomial case). Then you are in business. You can turn the Aho/Hopcroft/Ullman Euclidean algorithm's output into

$$ra + sm = 1.$$

This amounts to

$$ar = 1 - sm \equiv (-s)m + 1 \pmod{m}$$

So  $r$  is the  $b$  you were looking for, the reciprocal of  $a$  modulo  $m$ .

We have seen examples of hopeless searches for reciprocals above. There is no integer  $b$  such that

$$1255\ 5221b \equiv 1 \pmod{8\ 2530\ 7441}$$

because  $\gcd(1255\ 5221, 8\ 2530\ 7441) = 1\ 2593$ .

**Example 111.** The modulus  $m = 36$  provides an interesting case.

$$1 * 1 = 1 = 1 + 0 * 36 \equiv 1 \pmod{36} \quad i.e. \quad 1/1 = 1$$

$$5 * 29 = 145 = 1 + 4 * 36 \equiv 1 \pmod{36} \quad i.e. \quad 1/5 = 29$$

$$7 * 31 = 217 = 1 + 6 * 36 \equiv 1 \pmod{36} \quad i.e. \quad 1/7 = 31$$

$$11 * 23 = 253 = 1 + 7 * 36 \equiv 1 \pmod{36} \quad i.e. \quad 1/11 = 23$$

$$13 * 25 = 325 = 1 + 9 * 36 \equiv 1 \pmod{36} \quad i.e. \quad 1/13 = 25$$

$$17 * 17 = 289 = 1 + 8 * 36 \equiv 1 \pmod{36} \quad i.e. \quad 1/17 = 17$$

$$19 * 19 = 361 = 1 + 10 * 36 \equiv 1 \pmod{36} \quad i.e. \quad 1/19 = 19$$

$$(-1) * (-1) = 35 * 35 = 1225 = 1 + 34 * 36 \equiv 1 \pmod{36} \quad i.e. \quad 1/35 = 35$$

None of the other 24 remainders modulo 36 has a reciprocal modulo 36 (Why? Remember Euler's totient function.). Thus, in arithmetic modulo 36, we have

$$1 \equiv 1/1$$

$$5 \equiv 1/29,$$

$$29 \equiv 1/5$$

$$7 \equiv 1/31,$$

$$31 \equiv 1/7$$

$$11 \equiv 1/23,$$

$$23 \equiv 1/11$$

$$13 \equiv 1/25,$$

$$25 \equiv 1/13$$

$$17 \equiv 1/17$$

$$19 \equiv 1/19$$

$$-1 \equiv 35 \equiv 1/35 \equiv 1/(-1)$$

**Example 112.** There is no ordinary high school polynomial  $b(x)$  such that

$$(x^4 + 2x^3 - 2x^2 - 14x - 35)b(x) \equiv 1 \pmod{x^5 - 6x^3 + 3x^2 - 7x - 21}$$

because the  $gcd$  of those two polynomials is equal to  $x^2 - 7$ , according to Assertion 81. There is no polynomial  $b$  with coefficient arithmetic modulo 2 such that

$$1\ 0001 * b \equiv 1 \pmod{10\ 0111}$$

because the  $gcd$  of those two polynomials,  $1\ 0001$  and  $10\ 0111$ , is  $101$ . In other words the  $gcd$  of  $x^4 + 1$  and  $x^5 + x^2 + x + 1$  is  $x^2 + 1$  when the coefficient arithmetic is done modulo 2.

**Example 113.** Now let's consider some reciprocals which do exist, and let's find them. Find  $b$  such that  $7b \equiv 1 \pmod{23}$ . Well

remainders	quotients	copies of 23	copies of 7
23		1	-0
$\frac{23}{7}$	= 3+	-0	1
$\frac{2}{7}$	= 3+	1	-3
$\frac{1}{7}$	= 2 exactly	-3	10
$\frac{0}{7}$	is undefined	7	-23

So  $(-3)(23) + (10)7 = 1$ . In other words  $10 * 7 = 1 + 3 * 23$ . Thus  $7 * 10 \equiv 1 \pmod{23}$  in this first arithmetic.

**Example 114.** However, if you didn't mean that 7 and that 23, if you meant the octal abbreviation for the binary notation for polynomials with coefficient arithmetic modulo 2, then

remainders	quotients	copies of 23	copies of 7
23		1	0
$\frac{23}{7}$	= 6+	0	1
$\frac{1}{7}$	= 7+	1	6
$\frac{0}{7}$	is undefined	7	23

So  $1 * 23 + 6 * 7 = 1$ . In other words  $6 * 7 = 1 + 1 * 23$ . Thus  $7 * 6 \equiv 1 \pmod{23}$  in this second arithmetic.

**Example 115.** But maybe you didn't even mean that 7 and that 23. Maybe you meant the hex abbreviation for polynomials with coefficient arithmetic modulo 2. Then

remainders	quotients	copies of 23	copies of 7
23		1	0
$\frac{23}{7}$	= $D$ exactly	0	1
$\frac{0}{7}$	is undefined	1	$D$

So, in this case, 7 and 23 are not relatively prime. In fact  $23 = 7 * D$ . The task is thus impossible. 7 has no reciprocal modulo 23 in this third arithmetic.

It is a good exercise to verify the octal and hexadecimal computations above by working them out in binary.

12. A SECOND CUT AT NUMBER THEORY. THE DISTRIBUTION OF PRIMES.

**Theorem 121.** For any log symbol  $\sum_{p \leq N} \log(p)/p \sim \log(N)$ .

**Theorem 122.**  $\sum_{p \leq N} 1/p \sim \ln(\ln(N))$ .

**Theorem 123.**  $\pi(N) := \sum_{p \leq N} 1 \sim N/\ln(N)$ .

**Theorem 124.** The  $k$ th prime is  $\sim k \ln(k)$ .

**Theorem 125.** The density of primes near  $N$  is  $\sim 1/\ln(N)$ .

The average value of  $\varphi(N)/N$  is larger than  $3/5$ , *i.e.*

**Theorem 126.**  $\sum_{n \leq N} \varphi(n)/n \sim (6/\pi^2)N$ .

**Theorem 127.**  $\exists$  real  $A > 0 \ni \forall$  integer  $N \geq 4$

$$AN/\ln(\ln(N)) \leq \varphi(N) \leq N - 1.$$

See W.J. Leveque, Topics in Number Theory, Addison-Wesley, Reading, Massachusetts (1961), volumes I and II, or T.M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, New York (1976).

### 13. REDUCIBILITY AND IRREDUCIBILITY.

If the modulus  $m$  has no nontrivial factors, then the congruence  $ab \equiv 1 \pmod{m}$  can be solved for  $b$  unless  $b$  is a multiple of  $m$ , *i.e.* unless  $b \equiv 0 \pmod{m}$ . This is true whether  $m$  is an integer or a polynomial. An integer with no nontrivial factors is called a **prime**. A polynomial with no nontrivial factor is called **irreducible**. Thus

PRIME : INTEGER : : IRREDUCIBLE : POLYNOMIAL

COMPOSITE : INTEGER : : REDUCIBLE : POLYNOMIAL.

You have to watch your step when speaking about irreducible polynomials, though.

**Example 131.** The polynomial

$$x^2 - 1 = (x - 1) * (x + 1) = (x - 1)(x - [-1])$$

is **reducible** (*i.e.* not irreducible, since it obviously has a nontrivial factorization) **no matter what kind of coefficient arithmetic** you are doing.

The polynomial  $x^2 - 2$  is irreducible over the rationals.

**Example 132.** But  $x^2 - 2$  is reducible if you enlarge your viewpoint so as to allow real arithmetic. Here, the polynomial  $x^2 - 2$  factors

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}).$$

**Example 133.** Over the integers modulo 2, the polynomial  $x^2 - 2$  factors

$$x^2 - 2 = x^2 - 0 = x^2 = (x)(x) = (x - 0)(x - 0).$$

**Example 134.**  $x^2 - 2$  is irreducible over the integers modulo 3, or 4, or 5, or 6.

**Example 135.** But over the integers modulo 7, the polynomial  $x^2 - 2$  factors

$$x^2 - 2 = x^2 + 5 = (x - 4)(x - 3).$$

**Example 136.** Another polynomial,

$$x^2 + x + 1$$

is irreducible over the rationals.

**Example 137.**  $x^2 + x + 1$  is even irreducible over the reals.

**Example 138.** But if you allow for more possibilities by allowing complex number arithmetic,  $x^2 + x + 1$  becomes reducible with factorization

$$x^2 + x + 1 = (x - [-1/2 + i\sqrt{3}/2])(x - [-1/2 - \sqrt{3}/2]).$$

**Example 139.** Also,  $x^2 + x + 1$  is irreducible in modulo 2 coefficient arithmetic (we say it's irreducible over  $GF(2)$ ).

**Example 13A.** But if we let ourselves do coefficient arithmetic in a bigger structure,  $GF(4)$ , which contains  $GF(2)$  as a substructure, the polynomial  $x^2 + x + 1$  becomes reducible, with factorization  $x^2 + x + 1 = (x - 2)(x - 3)$ . As in Example 105 above, we remind the reader that the arabic symbols 2 and 3 used here are **not** the two and three of grammar school arithmetic. See Sections 14 and 15 below.

**Problem 131.** Do a high school arithmetic calculation with polynomials. Find  $b(x)$  such that

$$(x^3 + 27) * b(x) \equiv 1 \pmod{5x^4 + x^3 - 3x^2 + x + 7}$$

in high school arithmetic. Then see what it all means in arithmetic modulo 2.

#### 14. FIELDS, ESPECIALLY GALOIS FIELDS.

A field  $(F, +, 0, -, *1, /)$  is a set  $F$  of numbers which obey all the usual laws of the arithmetic of add, subtract, multiply and divide

$$a + b = b + a$$

$$a * b = b * a$$

$$a + (b + c) = (a + b) + c$$

$$a * (b * c) = (a * b) * c$$

$$a * (b + c) = (a * b) + (a * c)$$

$$a + 0 = a$$

$$a * 1 = a$$

$$a - a = 0$$

$$a/a = 1 \quad (\text{if } a \text{ is nonzero})$$

But though the laws hold, the facts are possibly unfamiliar. There are fields in which  $2 + 2 = 0$ . There is a field in which  $2 * 2 = 1$ , another in which  $7/6 = 3$ . For every number  $K$  on the following list, there is one (and only one) field with  $K$  elements

$$2, 3, 4, 5 \quad 7, 8, 9, \quad 11, \quad 13, \quad 16, 17, \quad 19, \quad 23, \quad 25, \dots .$$

But there are no fields of  $K$  elements if  $K$  is one of the numbers below

$$6, \quad 10, \quad 12, \quad 14, 15, \quad 18, \quad 20, 21, 22, \quad 24, \dots .$$

There is a field of size  $K$  if and only if  $K$  is a prime power  $p^N$ . The field with  $p^N$  elements is called  $GF(p^N)$ .

Figure 141 below tells what fields exist up to order 64.

The first column of the divide *op* table of every field is empty because you can't divide by zero.

**Example 142.** Here are the  $GF(5)$  *op* tables

		0	1	2	3	4
	+					
0		0	1	2	3	4
1		1	2	3	4	0
2		2	3	4	0	1
3		3	4	0	1	2
4		4	0	1	2	3

		0	1	2	3	4
	-					
0		0	4	3	2	1
1		1	0	4	3	2
2		2	1	0	4	3
3		3	2	1	0	4
4		4	3	2	1	0

		0	1	2	3	4
	*					
0		0	0	0	0	0
1		0	1	2	3	4
2		0	2	4	1	3
3		0	3	1	4	2
4		0	4	3	2	1

		0	1	2	3	4
	/					
0		.	0	0	0	0
1		.	1	3	2	4
2		.	2	1	4	3
3		.	3	4	1	2
4		.	4	2	3	1

Here's an instant replay of the  $GF(5)$  multiplication table.

		0	1	2	4	3
	*					
0		0	0	0	0	0
1		0	1	2	4	3
2		0	2	4	3	1
4		0	4	3	1	2
3		0	3	1	2	4

Do you prefer this way or the other way of summarizing multiplication? Why?

A moment's reflection will show that  $GF(5)$  arithmetic is just arithmetic modulo 5.

We are especially interested in the fields  $GF(2^N)$ , *i.e.* the field with two members, the field with four, the field with eight, . . . .

**Example 141.** Here are the facts for  $GF(2)$ , the operation tables

	0	1		0	1		0	1		0	1
	+			-			*			/	
0	0	1	0	0	1	0	0	0	0	.	0
1	1	0	1	1	0	1	0	1	1	.	1

Note the Orwellian feature of  $GF(2)$  arithmetic: PLUS IS MINUS. Note, also, that + amounts to XOR (logical “exclusive or” of truth values), and that \* amounts to logical AND of truth values. Note, finally, that  $GF(2)$  arithmetic is arithmetic modulo 2.

**Example 143.**  $GF(4)$  arithmetic is not arithmetic modulo 4. Here are the  $GF(4)$  op tables. Unlike  $GF(5)$ ,  $GF(4)$  is Orwellian: PLUS IS MINUS. So we omit the subtraction table.

	0	1	2	3		0	1	2	3		0	1	2	3
	+					*					/			
0	0	1	2	3	0	0	0	0	0	0	.	0	0	0
1	1	0	3	2	1	0	1	2	3	1	.	1	3	2
2	2	3	0	1	2	0	2	3	1	2	.	2	1	3
3	3	2	1	0	3	0	3	1	2	3	.	3	2	1

**Fact 141.** The arithmetic of  $GF(p)$  is **always arithmetic modulo  $p$**  if  $p$  is prime.

**Fact 142.** The arithmetic of  $GF(p^N)$  is **never arithmetic modulo  $p^N$**  if  $N$  is bigger than 1.

**Example 144.**  $GF(8)$  arithmetic is very different from arithmetic modulo 8. Here are the  $GF(8)$  *op* tables. Unlike  $GF(5)$ , the field  $GF(8)$  is Orwellian: PLUS IS MINUS. So we omit the subtraction table.

		0	1	2	3	4	5	6	7			0	1	2	3	4	5	6	7	
	+										*									
0		0	1	2	3	4	5	6	7	0		0	0	0	0	0	0	0	0	0
1		1	0	3	2	5	4	7	6	1		0	1	2	3	4	5	6	7	7
2		2	3	0	1	6	7	4	5	2		0	2	4	6	3	1	7	5	5
3		3	2	1	0	7	6	5	4	3		0	3	6	5	7	4	1	2	2
4		4	5	6	7	0	1	2	3	4		0	4	3	7	6	2	5	1	1
5		5	4	7	6	1	0	3	2	5		0	5	1	4	2	7	3	6	6
6		6	7	4	5	2	3	0	1	6		0	6	7	1	5	3	2	4	4
7		7	6	5	4	3	2	1	0	7		0	7	5	2	1	6	4	3	3

		0	1	2	3	4	5	6	7
	/								
0		·	0	0	0	0	0	0	0
1		·	1	5	6	7	2	3	4
2		·	2	1	7	5	4	6	3
3		·	3	4	1	2	6	5	7
4		·	4	2	5	1	3	7	6
5		·	5	7	3	6	1	4	2
6		·	6	3	2	4	7	1	5
7		·	7	6	4	3	5	2	1

This is not a particularly revealing or economical way to display the true nature of  $GF(8)$  arithmetic. See Figure 152 for a more economical, more revealing way.

---

order (size)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	
number	0	0	1	1	1	1	0	1	1	1	0	1	0	1	

  

order (size)	14	15	16	17	18	19	20	21	22	23	24	25	26	
number	0	0	1	1	0	1	0	0	0	1	0	1	0	

  

order (size)	27	28	29	30	31	32	33	34	35	36	37	38	
number	1	0	1	0	1	1	0	0	0	0	1	0	

  

order (size)	39	40	41	42	43	44	45	46	47	48	49	50	
number	0	0	1	0	1	0	0	0	1	0	1	0	

  

order (size)	51	52	53	54	55	56	57	58	59	60	61	62	63	64	
number	0	0	1	0	0	0	0	0	1	0	1	0	0	1	

**Figure 141.** A table of how many Galois fields there are of each order from 0 to 64.

---

## 15. SMART DISPLAYS OF TABLES FOR SMALL GALOIS FIELDS.

The op tables in Section 14 above are wasteful of space. So we tighten up the displays. The margins of the  $+$  and  $*$  tables can be removed since they coincide with first rows and columns. The negatives and reciprocals are enough to yield subtraction and division by setting

$$a - b := a + (-b),$$

$$a/b := a^{-1} * b.$$

Then the finite fields smaller than  $GF(11)$  are described in the smart displays shown in Figures 151 and 152 below.

Note that a careful choice of ordering for elements in the (now invisible) margins of the multiplication table leads, in every case  $q$  less than 11, to a  $GF(q)$  multiplication table with the distinctive regimental stripe pattern characteristic of a cyclic group (namely  $C_{q-1}$  in each case above), and with bottom and right borders consisting of zeros.

Note, also, that the addition tables resemble checkerboards whose squares are regimental stripes. This is the way the table of a product of copies of a cyclic group looks.

**Question 151.** Is the additive group of  $GF(p^N)$  a product

$$C_p \times C_p \times \cdots \times C_p$$

of  $N$  cyclic groups of order  $p$ ?

**Question 152.** Is the multiplicative group of nonzero elements of  $GF(p^N)$  the cyclic group  $C_s$ , where  $s = -1 + p^N$ ?

		$(GF(2))$		
-	+		-1	*
0	0 1		1	1 0
1	1 0		no	0 0
		$(GF(3))$		
-	+		-1	*
0	0 1 2		1	1 2 0
2	1 2 0		2	2 1 0
1	2 0 1		no	0 0 0
		$(GF(4))$		
-	+		-1	*
0	0 1 2 3		1	1 2 3 0
1	1 0 3 2		3	2 3 1 0
2	2 3 0 1		2	3 1 2 0
3	3 2 1 0		no	0 0 0 0
		$(GF(5))$		
-	+		-1	*
0	0 1 2 3 4		1	1 2 4 3 0
4	1 2 3 4 0		3	2 4 3 1 0
3	2 3 4 0 1		4	4 3 1 2 0
2	3 4 0 1 2		2	3 1 2 4 0
1	4 0 1 2 3		no	0 0 0 0 0
		$GF(6)$	does not exist.	

**Figure 151.** The four smallest Galois fields.

$(GF(7))$

-	+									-1	*
0		0	1	2	3	4	5	6		1	1 3 2 6 4 5 0
6		1	2	3	4	5	6	0		5	3 2 6 4 5 1 0
5		2	3	4	5	6	0	1		4	2 6 4 5 1 3 0
4		3	4	5	6	0	1	2		6	6 4 5 1 3 2 0
3		4	5	6	0	1	2	3		2	4 5 1 3 2 6 0
2		5	6	0	1	2	3	4		3	5 1 3 2 6 4 0
1		6	0	1	2	3	4	5		no	0 0 0 0 0 0 0

$(GF(8))$

-	+										-1	*
0		0	1	2	3	4	5	6	7		1	1 2 4 3 6 7 5 0
1		1	0	3	2	5	4	7	6		5	2 4 3 6 7 5 1 0
2		2	3	0	1	6	7	4	5		7	4 3 6 7 5 1 2 0
3		3	2	1	0	7	6	5	4		6	3 6 7 5 1 2 4 0
4		4	5	6	7	0	1	2	3		3	6 7 5 1 2 4 3 0
5		5	4	7	6	1	0	3	2		4	7 5 1 2 4 3 6 0
6		6	7	4	5	2	3	0	1		2	5 1 2 4 3 6 7 0
7		7	6	5	4	3	2	1	0		no	0 0 0 0 0 0 0 0

$(GF(9))$

-	+										-1	*
0		0	1	2	3	4	5	6	7	8	1	1 4 6 7 2 8 3 5 0
2		1	2	0	4	5	3	7	8	6	5	4 6 7 2 8 3 5 1 0
1		2	0	1	5	3	4	8	6	7	3	6 7 2 8 3 5 1 4 0
6		3	4	5	6	7	8	0	1	2	8	7 2 8 3 5 1 4 6 0
8		4	5	3	7	8	6	1	2	0	2	2 8 3 5 1 4 6 7 0
7		5	3	4	8	6	7	2	0	1	7	8 3 5 1 4 6 7 2 0
3		6	7	8	0	1	2	3	4	5	6	3 5 1 4 6 7 2 8 0
5		7	8	6	1	2	0	4	5	3	4	5 1 4 6 7 2 8 3 0
4		8	6	7	2	0	1	5	3	4	no	0 0 0 0 0 0 0 0

**Figure 152.** The next three smallest Galois fields.

For  $GF(2^N)$ , it is possible to give even terser descriptions of arithmetic.

For every  $N$ ,  $+$  is just XOR (bitwise exclusive or, in other words, modulo two entrywise addition – without carry – of lists of  $N$  zeros and ones). And  $-$  is also XOR.  $+$  and  $-$  are independent of the choice of irreducible (over  $GF(2)$ ) polynomial  $\pi(x)$ . For our  $GF(4)$  above, we merely write

$$(2^0, 2^1, 2^2) = (1, 2, 3)$$

and the entire multiplicative structure follows. For our  $GF(8)$  above, we merely write

$$(2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6) = (1, 2, 4, 3, 6, 7, 5)$$

and the entire multiplicative structure follows. In general for  $GF(2^N)$  it suffices to say

$+$  is XOR

$-$  is XOR

$$(g^0, g^1, g^2, \dots, g^{2^N-2}) = (1, g, \dots)$$

$$(g^t)^{-1} = g^{2^N-1-t}$$

*i.e.* to list the successive powers of a generator  $g$  of the multiplicative group. Even this becomes too tedious if  $N \geq 2^{120} \geq 10^{36}$  because the list is (way) too long to store. Display on paper ceases to be possible.

On a general-purpose computer, for  $N \geq 30$  (and, indeed, usually for all  $N$ ), people just use XOR for  $+$  and  $-$ , use Cauchy multiplication, followed by reduction mod  $\pi(x)$  for  $*$ , and use the Euclidean algorithm to calculate  $b^{-1}$ , and then form the quotient  $a/b = ab^{-1}$ . On a high-powered PC, a single inverse (*i.e.* reciprocal) can take seconds if  $N \geq 1000$ .

On special-purpose hardware, **linear feedback shift registers** (LFSRs) can be employed. Here it is possible to work with  $N$  so large that a general purpose computer is impractical.

## 16. GALOIS FIELDS.

At this point we must build the arithmetic of  $GF(p^N)$ . To do so, it is worthwhile to consider polynomials whose coefficient arithmetic is arithmetic modulo a prime  $p$ . Thus the coefficient arithmetic is wrapped around  $p$ . But the polynomial arithmetic will then also be wrapped around an irreducible polynomial  $\pi(x)$ . And there should be strict adherence to Principle 101. As soon as there is an opportunity to reduce mod  $p$ , do so. Never perform any reduction mod  $\pi(x)$  while a reduction mod  $p$  is available. And even in the course of a reduction mod  $\pi(x)$ , reduce mod  $p$  as early as possible in each ancillary computation.

Let  $p$  be a prime, and let  $N$  be a positive integer. Let  $\pi(x)$  be an irreducible polynomial of degree  $N$  over  $GF(p)$  (which you can regard as being  $\mathbb{Z}/p\mathbb{Z}$ , or as being  $\mathbb{C}_p$ ).

**Definition 161.**  $GF(p^N)$  is the set of residue classes modulo  $\pi(x)$  of the ring  $(\mathbb{Z}/p\mathbb{Z})[x]$  of polynomials over  $\mathbb{Z}/p\mathbb{Z}$ .

**Comment 161.** The residue classes of Definition 131 are in one-to-one correspondence with the polynomials of degree less than  $N$  over  $\mathbb{Z}/p\mathbb{Z}$ , *i.e.* with the set of lists  $(a_0, a_1, \dots, a_{N-1})$  of  $N$  elements of  $\mathbb{Z}/p\mathbb{Z}$ . Since  $\mathbb{Z}/p\mathbb{Z}$  has  $p$  members, it follows that  $GF(p^N)$  has  $p^N$  members.

**Theorem 161.**  $GF(p^N)$  is a field for every prime  $p$ , every positive integer  $N$ .

**Proof:** An easy exercise.

**Theorem 162.** Suppose that  $\mathbb{F}$  is a field with finitely many elements, say  $q$  elements. Then there is a prime  $p$  and a positive integer  $N$  such that  $q = p^N$ . Moreover  $\mathbb{F}$  is isomorphic to  $GF(p^N)$ .

**Proof:** Iain T. Adamson, *Introduction to Field Theory*, Second Edition, Cambridge University Press (1982), p. 127.

**Theorem 163.** If  $\mathbb{F}$  and  $\mathbb{G}$  are fields of size  $q$  there is a way to construct an isomorphism between them.

Let  $q$  and  $r$  be positive integers. If  $GF(q)$  contains subfields isomorphic to  $GF(r)$ , how many such subfields does it contain?

It contains none if  $q$  is not a power of  $r$ . It contains **exactly one** such subfield when  $q$  is a power of  $r$ .

More exactly

**Theorem 164.**  $GF(r)$  is isomorphic to a subfield of  $GF(q)$  if and only if there is a prime  $p$ , and there are positive integers  $A$  and  $B$  such that

$$\begin{aligned} r &= p^A \\ q &= p^{AB}. \end{aligned}$$

If  $GF(r)$  is isomorphic to each of two subfields  $\mathbb{K}$  and  $\mathbb{L}$  of  $GF(q)$  then  $\mathbb{K} = \mathbb{L}$ . Suppose  $r = p^A$ , and that  $q = p^{AB}$ . Suppose that  $\mathbf{i}$  is an isomorphism from the field

$$(GF(r), +, -, \times, ^{-1}, 0, 1)$$

onto the subfield

$$(\mathbb{K}, +, -, \times, \mathbf{rec}, \theta, v)$$

of  $(GF(q), +, -, \times, \mathbf{rec}, \theta, v)$ . Suppose that  $g$  is a generator of the multiplicative group of  $GF(r) = GF(p^A)$ . This means that the multiplicative order of  $g$  is  $p^A - 1$ . Suppose that  $\gamma$  is a generator of the multiplicative group of  $GF(q) = GF(p^{AB})$ . This means that the multiplicative order of  $\gamma$  is

$$(p^{AB} - 1) = (p^A - 1)(p^{A(B-1)} + p^{A(B-2)} + \dots + p^{2A} + p^A + 1) = (p^A - 1)\sigma.$$

Then every one of the  $p^A - 1$  nonzero elements  $e$  of  $\mathbb{K}$  is of the form

$$e = \gamma^{\sigma j}$$

where

$$\sigma = p^{A(B-1)} + p^{A(B-2)} + \dots + p^{2A} + p^A + 1$$

and  $j \in \{0, 1, 2, \dots, p^A - 2, p^A - 1\}$ . And the isomorphism  $\mathbf{i}$  is of the form

$$\begin{aligned} \mathbf{i}(0) &= v \\ \mathbf{i}(g^j) &= \gamma^{\sigma j} \end{aligned}$$

for some generator  $g$  of the multiplicative group of  $GF(p^A)$ , some generator  $\gamma$  of the multiplicative group of  $GF(p^{AB})$ . It follows that

$$\mathbf{i}(1) = v$$

for any such  $g$ , any such  $\gamma$ .

Thus there can be several monomorphisms  $\mathbf{i}: GF(p^A) \rightarrow GF(p^{AB})$ . But the image  $\mathbf{i}(GF(p^A))$  is independent of  $\mathbf{i}$ . It is the only subfield of  $GF(p^{AB})$  whose order is  $p^A$ .

**Fact 161.** Suppose that  $-1 + 2^p$  is a Mersenne prime. Then every element of the Galois field  $GF(2^p)$  – other than 0 or 1 – is a **primitive element** (*i.e.* is a generator of the multiplicative group of that field).