10.4

Finite Fields

P. Danziger

1 The Modular Congruence Relation (Review)

For a positive fixed integer n we define $a \bmod n$ to be the remainder of a when divided by n. Note that $a \bmod n$ always yields a number less than n
C and Java use % to denote mod, i.e. $a \,\%\, b$ means $a \bmod b$
On the other hand we have the equivalence class of integers modulo n.
Thus for any integers a, b and n,

$$a \equiv b \pmod{n} \quad \text{if and only if} \quad (a \bmod n) = (b \bmod n).$$

Notes

1. $a \bmod n$ is always an integer less than n, but the a and b in $a \equiv b \pmod{n}$ can be any integers.
2. $a \equiv b \pmod{n}$ if and only if $n \,|\, (a - b)$.

Example 1

1. Congruence modulo 2, take $n = 2$.
   $a = 0 \bmod 2$ if and only if $a = 2m$ for some $m \in \mathbb{Z}$, i.e. a is even.
   So all even numbers are congruent to each other modulo 2.
   $a = 1 \bmod 2$ if and only if $a = 2m + 1$ for some $m \in \mathbb{Z}$, i.e. a is odd.
   So all odd numbers are congruent to each other modulo 2.

   eg. $158 \equiv 14 \pmod 2$, and $1231 \equiv 121 \pmod 2$.

   But $158 = 0 \bmod 2$ and $1231 = 1 \bmod 2$.

2. Congruence modulo 4, take $n = 4$.
   The members of the following sets are all congruent to each other modulo 4:

   $0 \pmod 4$:
   $\{x \in \mathbb{Z} \,|\, \exists\, m \in \mathbb{Z} \text{ such that } x = 4m\} = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$,
   So $-12 \equiv -8 \equiv -4 \equiv 0 \equiv 4 \equiv 8 \equiv 12 \pmod 4$.

   $1 \pmod 4$:
   $\{x \in \mathbb{Z} \,|\, \exists\, m \in \mathbb{Z} \text{ such that } x = 4m + 1\} = \{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\}$,
   So $-11 \equiv -7 \equiv -3 \equiv 1 \equiv 5 \equiv 9 \equiv 13 \pmod 4$.

   $2 \pmod 4$:
   $\{x \in \mathbb{Z} \,|\, \exists\, m \in \mathbb{Z} \text{ such that } x = 4m + 2\} = \{\ldots, -10, -6, -2, 2, 6, 10, 14, \ldots\}$,
   So $-10 \equiv -6 \equiv -2 \equiv 2 \equiv 6 \equiv 10 \equiv 14 \equiv \pmod 4$

   $3 \pmod 4$:
   $\{x \in \mathbb{Z} \,|\, \exists\, m \in \mathbb{Z} \text{ such that } x = 4m + 3\} = \{\ldots, -9, -5, -1, 3, 7, 11, 15, \ldots\}$.
   So $-9 \equiv -5 \equiv -1 \equiv 3 \equiv 7 \equiv 11 \equiv 15 \pmod 4$.

3. Congruence modulo 6, let $n = 6$,
   $1 \equiv 7 \equiv 13 \equiv 19 \equiv 25 \equiv \ldots \pmod 6$

2 Modular Arithmetic

We may do arithmetic on the equivalence class of integers modulo n. In this case we treat different elements of the same modular class equivalently, though we usually use the smallest positive integer in a class as its representative. The reason we can do this is the following theorem.

2.1 Addition

Theorem 2 *For a given fixed integer n and any $a, b \in \mathbb{Z}$*

$$(a \bmod n) + (b \bmod n) = (a + b) \bmod n$$

This theorem means that we can take any representative of a modular class and use it in modular addition. Further, all the usual algebraic rules for addition and subtraction are inherited by modular arithmetic.
This allows us to define addition "modulo n" by $a + b \pmod n = (a + b) \bmod n$.
Perhaps the most important consequence is the rule of Cancellation for modular addition.

Theorem 3 *Given integers a, b, c and n, with $n > 1$,*

$$a + c \equiv b + c \Leftrightarrow a \equiv b \pmod n$$

Proof: Let $a, b, c, n \in \mathbb{Z}$, with $n > 1$.

($\Rightarrow$) Suppose that $a + c \equiv b + c \pmod n$.
Thus $n \mid ((a + c) - (b + c))$. $(x \equiv y \pmod n \Leftrightarrow n \mid x - y)$
So $n \mid (a - b)$, and hence $a \equiv b \pmod n$. $(x \equiv y \Leftrightarrow n \mid x - y)$

($\Leftarrow$) Suppose that $a \equiv b \pmod n$.
Thus $n \mid (a - b)$. $(x \equiv y \pmod n \Leftrightarrow n \mid x - y)$
So $n \mid ((a + c) - (b + c))$. $(c - c = 0)$
So $a + c \equiv b + c \pmod n$. $(x \equiv y \pmod n \Leftrightarrow n \mid x - y)$ $\square$

Example 4

1. Let $n = 5$.
   $8 + 11 \equiv 4 \pmod 5$, $13 + 7 \equiv 0 \pmod 5$, $3 + 3 = 1 \pmod 5$, etc.
   $13 + 9 + 11 \equiv (((13 + 9) \bmod 5) + 11) \equiv 2 + 1 \equiv 3 \pmod 5$,
   $3 + 4 + 1 \equiv (3 + ((4 + 1) \bmod 5) \equiv 3 + 0 \equiv 3 \pmod 5$.
   Note how we can take mod at any point in the calculation without effect on the final answer.
2. Find x such that $x + 3 \equiv 1 \pmod 7$.
   $x + 3 \equiv 1 \bmod 7 \Rightarrow x \equiv 1 - 3 \equiv -2 \equiv 5 \pmod 7$

Since there are a finite number of possibilities we may write down the table of addition.

Example 5
For example, addition modulo 5:

$+ \bmod 5$	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

Addition mod 5

Notation We use $\mathbb{Z}_n$ to denote the set of integers from 0 to $n-1$, together with the operation of addition modulo n.

Theorem 6 *Addition modulo n satisfies all of the following:*

Closure For all $a, b \in \mathbb{Z}_n$, $(a+b \pmod n) \in \mathbb{Z}_n$.

Associativity For all $a, b, c \in \mathbb{Z}_n$, $(a+b)+c \equiv a+(b+c) \pmod n$.

Existence of Identity There exist an element of $\mathbb{Z}_n$, denoted 0, such that for every $a \in \mathbb{Z}$, $a+0 \equiv 0+a \equiv a \pmod n$.

Existence of Inverse For every $a \in \mathbb{Z}_n$, there exists $-a \in \mathbb{Z}_n$, called the *additive inverse of a,* such that $a+(-a) \equiv (-a)+a \equiv 0 \pmod n$.

Definition 7 *Given a set S and a binary operation '+' defined on S if + satisfies the above axioms $(S,+)$ is called a group. If it also satisfies commutativity below it is called a commutative group or an Abelian group.*

Commutativity For all $a, b \in \mathbb{Z}_n$, $a+b \equiv b+a \pmod n$

We can find the additive inverse of $a \in \mathbb{F}_n$ by considering what we would have to add to a to get $0 \bmod n$, which is $n \bmod n$. ie $n-a = -a \bmod n$.

Example 8
Take $n = 5$.

a	0	1	2	3	4
$-a$	-0	-1	-2	-3	-4
$-a \bmod 5$	0	4	3	2	1

So, for example, $2+3 = 0 \bmod 5$, so $3 \equiv -2 \pmod 5$ and $2 \equiv -3 \pmod 5$.

2.2 Multiplication

We can also define multiplication modulo n in a similar way:

Theorem 9 *For a given fixed integer n and any $a, b \in \mathbb{Z}$*

$$(a \bmod n) \times (b \bmod n) = (a \times b) \bmod n$$

Example 10
Let $n = 5$.
$3 \times 1 \equiv 3 \pmod 5$, $3 \times 2 \equiv 1 \pmod 5$, $3 \times 3 \equiv 4 \pmod 5$, etc.
$3 \times 4 \times 2 \equiv (((3 \times 4) \bmod 5) \times 2) \equiv 2 \times 2 \equiv 4 \pmod 5$.
$13 \times 9 \times 22 \equiv (((3 \times 4) \bmod 5) \times 22) \equiv 2 \times 2 \equiv 4 \pmod 5$.
Once again by taking mod n after each operation we can keep the size of the operands manageable (less than n).
In a similar manner to addition we may write down the table of multiplication modulo 5:

$\times \bmod 5$	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

Multiplication mod 5

For the moment we will use S_n to denote the integers from 1 to $n-1$, i.e. $S_n = \{1, 2, 3, \ldots, n-1\}$
We would like to say that the operation of $\times$ on S_n is a group. It satisfies closure, associativity and commutativity above. In addition, since we exclude 0 from our set, there is an identity, namely 1. However, there is a problem with inverses. Consider the case where $n = 6$:

x		1	2	3	4	5
$2x$	$\pmod 6$	2	4	0	2	4

There is no $x \in S_6$ such that $2x = 1$. Further $2 \times 3 \equiv 0 \pmod 6$, so there are "zero divisors". Thus division is not well defined: is $4/2 \equiv 2$ or $5 \pmod 6$? In fact these problems are related. Saying that there are $a, b \in S_n$ such that $ab = 0 \bmod n$ is just saying that a and b are factors of n. The problem is more subtle though, consider 6 mod 10. $6 \times 5 \equiv 0 \pmod{10}$, so 6 is a zero divisor of 10, but it does not divide 10. It turns out that a has a multiplicative inverse modulo n exactly when they are relatively prime, i.e. $\gcd(a, n) = 1$.
Suppose that a, b and n are integers with the property that $ab \equiv 1 \pmod n$ then by the definition of mod there exists $k \in \mathbb{Z}$ such that $ab = 1 + kn$, or $ab - kn = 1$. We thus will find the following result useful.

Theorem 11 (Linear Combination of Integers (10.4.5)) *For all integers a and b, not both zero, if $d = \gcd(a, b)$, then there exist integers s and t such that $d = as + bt$.*

SWP

Corollary 12 (Existence of Multiplicative Inverses (10.4.6)) *Given $n \in \mathbb{Z}$, with $n > 1$, and $a \in S_n$ with a and n relatively prime, so $gcd(a, n) = 1$, then there exists $b \in S_n$, called the* multiplicative inverse of a, *such that $ab \equiv ba \equiv 1 \pmod{n}$. We write a^{-1} for b.*

If n has no factors (i.e. n is prime) all integers will be relatively prime to it and division will be well defined.

Corollary 13 *If p is a prime, then for every $a \in S_p$, there exists $b \in S_p$, called the* multiplicative inverse of a, *such that $ab \equiv ba \equiv 1 \pmod{p}$. We write a^{-1} for b.*

This means that in the case where n is a prime multiplication is a group on S_n and division is well defined.
In order to show that the cancellation theorem holds we will need the following Lemma.

Theorem 14 (Euclids Lemma) *For all integers a, b and c if $\gcd(a, c) = 1$ and $a \mid bc$ then $a \mid b$.*

Proof: Let $a, b, c \in \mathbb{Z}$, with $\gcd(a, b) = 1$ and $a \mid bc$.
Since $a \mid bc$ there exists $k \in \mathbb{Z}$ such that $bc = ka$.
Since $\gcd(a, b) = 1$, by the Linear Combination Theorem there exist integers s and t such that $as + ct = 1$.

$$\begin{aligned} b &= bas + bct && \text{(multiplying through by } b\text{)} \\ &= bas + kat && \text{(Substitution } bc = ka\text{)} \\ &= a(bs + kt) && \text{(Distributivity)} \end{aligned}$$

Now, $bs + kt \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under $+$ and $\times$, so $a \mid b$. $\square$

Theorem 15 (Cancellation Theorem) *For all integers a, b, c and n, if $\gcd(c, n) = 1$ and $ac \equiv bc \pmod{n}$ then $a \equiv b \pmod{n}$.*

Proof: Let $a, b, c, n \in \mathbb{Z}$, with $\gcd(c, n) = 1$ and $ac \equiv bc \pmod{n}$.
Since $ac \equiv bc \pmod{n}$ we know that $ac - bc \equiv 0 \pmod{n}$.
So $c(a - b) \equiv 0 \pmod{n}$, or equivalently $n \mid c(a - b)$.
But $\gcd(c, n) = 1$, so by Euclid's Lemma we must have that $n \mid (a - b)$.
Which is equivalent to saying $a \equiv b \pmod{n}$ by the definition of $\pmod{}$ $\square$
Note that the Cancellation Theorem says the usual rule of cancellation works for every member of the field. However, it is more general, in that it works for any element in a non field that has an inverse. The cancellation rule is also known as "multiplying on both sides" of an equation.

Example 16

1. Solve the equation $2x = 3 \pmod{5}$ for x.

$2^{-1} = 3 \pmod{5}$, from the table, so

$$\begin{aligned} & 2x \equiv 3 && \pmod{5} && \text{(Given)} \\ \Rightarrow\ & 2^{-1} \cdot 2x \equiv 2^{-1} \cdot 3 && \pmod{5} && \text{(Muliplying both sides by } 2^{-1}\text{)} \\ \Rightarrow\ & x \equiv 3 \cdot 3 && \pmod{5} && (2^{-1} = 3, \text{ and definition of inverse}) \\ \Rightarrow\ & x \equiv 9 && \pmod{5} \\ \Rightarrow\ & x \equiv 4 && \pmod{5} \end{aligned}$$

2. Find x such that $3x + 2 \equiv 1 \pmod 5$.

$$\begin{array}{rcll} 3x+2 & \equiv & 1 & \pmod 5 \quad \text{(Given)} \\ 3x & \equiv & 1-2 & \pmod 5 \quad \text{(Cancellation Rule for Addition)} \\ x & \equiv & 3^{-1} \times -1 & \pmod 5 \quad \text{(Cancellation Rule for Multiplication)} \\ x & \equiv & -2 & \pmod 5 \quad (3^{-1} \equiv 2 \pmod 5) \\ x & \equiv & 3 & \pmod 5 \quad (-2 \equiv 3 \pmod 5) \end{array}$$

3. Find x such that $x^2 \equiv 1 \pmod 5$.

   Perusal of the multiplication table mod 5 gives that $4 \times 4 \equiv 1 \pmod 5$. Note that $x = 1$ is also a solution. So $x = 1$ or 4.

2.3 Finite Fields

If a set S has a binary operation $(\oplus)$ defined on it with identity $0 \in S$ and another binary operation on $S \setminus \{0\}$ $(\otimes)$, $(S, \oplus, \otimes)$ is called a field if these two operations are both groups and also satisfy the distributive laws below. For all a, b and $c \in S$:

D1 $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$.

D2 $(b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)$.

The set $\{0, 1, 2, \ldots, p-1\}$, where p is a prime with addition and multiplication modulo p is a field. We denote this field by $\mathbb{F}_p$.

2.3.1 Prime Power Fields

If $q = p^\alpha$ is a power of a prime it is possible to define a multiplication operation that satisfies all of the group axioms. This gives rise to prime power fields.

Example 17
$q = 4 = 2^2$. Addition is defined as usual mod p, multiplication is now given by the table below.

$\otimes$ in 2^2	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Multiplication in 2^2

Note that the multiplication given here is **not** modular multiplication, but does satisfy the field axioms. We will not consider such fields further in this course. All fields from now on will be either $\mathbb{R}$ or $\mathbb{F}_p$ for some prime p, however most of the ideas herein are the same for any field.

2.3.2 Binary

A case worthy of special attention is when $p = 2$, $\mathbb{F}_2$ - binary arithmetic.

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Binary addition is equivalent to the logical operation of XOR and binary multiplication is equivalent to the logical operation of AND.
In particular note that $1 + 1 = 0$, and so $-1 = 1$.

$$0 - 0 = 0, \qquad 1 - 1 = 0, \qquad 1 - 0 = 1, \qquad 0 - 1 = 1.$$

We also have the corresponding operation of *binary division*:

$$\frac{1}{1} = 1, \qquad \frac{0}{1} = 0.$$

Exercises 1

1. Find the following. In each case you answer should be an integer between 0 and 4. (Hint there's an easy way to find the value of any integer mod 5)
   (a) $5 + 4 \bmod 5$
   (b) $12384423344 + 2344872309 \bmod 5$
   (c) $12384423344 + 2344872309 + 2 \bmod 5$
   (d) $3 - 4 \bmod 5$
   (e) $-7 \bmod 5$
   (f) $15 - 7 \bmod 5$
   (g) $134857908752 - 954871451098754 \bmod 5$
2. Find the following. In each case you answer should be an integer between 0 and 4.
   (a) $3 \times 2 \pmod 5$
   (b) $5 \times 4 \pmod 5$
   (c) $3 \times (-2) \pmod 5$
   (d) $3 \times (-2) \pmod 5$
   (e) $134857908752 \times 954871451098754 \pmod 5$
3. Find the following. In each case you answer should be an integer between 0 and 4. You will need to use the multiplication table for mod 5 on page 4 to find inverses.
   (a) $a^{-1} \pmod 5$ for each $a \in \{1, 2, 3, 4\}$

(b) $3 \cdot 2^{-1} \pmod 5$.

(c) $1/3 \pmod 5$

(d) $\frac{134857908752}{54871451098754} \pmod 5$

(e) Is $2 \times 4^{-1} \equiv 1 \times 2^{-1} \pmod 5$? i.e. is $\frac{2}{4} \equiv \frac{1}{2} \pmod 5$?

4. Find x in each case below.

(a) $3x + 2 \equiv 4 \pmod 5$.

(b) $6x + 17 \equiv 14 \pmod 5$.

(c) $273727x + 302039 \equiv 387232 \pmod 5$.

(d) $x/3 + 12 \equiv 23 \pmod 5$

5. Verify that the prime power Field in example 2.3.1 satisfies D1 and D2 on page 6 in the following cases:

(a) $(a, b, c) = (0, 2, 1)$

(b) $(a, b, c) = (3, 2, 1)$

(c) $(a, b, c) = (2, 1, 1)$

3 Multiplicative Inverses

The statement that multiplicative inverses exist is all very well, but they seem to be difficult to find. In this section we investigate some of these difficulties and try to find ways around them.
We can find the multiplicative inverse of $a \in \mathbb{F}_p$ by finding $b \in \mathbb{F}_p$ such that $ab \equiv 1 \pmod p$. This can be done by finding integer solutions to the equation $ax = 1 + py$ or equivalently $ax - py = 1$. We are only interested in x, since this gives us $b \equiv x \pmod p$. Equations of this form $(ax - py = 1)$ are known as *Diophantine equations.*

3.1 Brute Force

We first try a brute force approach to finding inverses. This can somnetimes be effective, especially for small fields.

Example 18
If $p = 5$ we may work from the table above. Given x, we look along the row for x, until we find the column y such that $xy = 1$.
Thus $2^{-1} \equiv 3$, $3^{-1} \equiv 2$ and $4^{-1} \equiv 4 \pmod 5$.
Note that for large primes finding multiplicative inverses by this method can be non-trivial, since we may have to check up to p possibilities for each inverse.

3.2 Diophantine equations

We wish to find integer solutions to equations of the form $ax - py = 1$, where p is a prime.
Recall the Euclidean Algorithm for finding $\gcd(a, b)$
int $\gcd(a, b)$ {
If $a = b = 0$, (no gcd) return ERROR.
If $a = b$ return a.
If $a = 0$ return b.
If $b = 0$ return a.
If $a > b$ return $\gcd(b, a \bmod b)$.
Else return $\gcd(a, b \bmod a)$.
}
Now since p is prime we know that $\gcd(a, p) = 1$, we may obtain a solution to $ax - py = 1$ by running the Euclidean algorithm and then reversing back up the steps from 1.

Example 19

1. To find $4^{-1} \bmod 17$ we must find integers x and y such that $4x + 17y = 1$.

$$\gcd(17, 4) \qquad 17 = 4 \cdot 4 + 1 \qquad \therefore 1 = 17 - 4 \cdot 4$$

   So take $x = -4$ and $y = 1$. Now $-4 = 13 \bmod 17$, so $4^{-1} = 13 \bmod 17$

2. To find $5^{-1} \bmod 17$ we must find integers x and y such that $5x + 17y = 1$.

$$\begin{array}{ll} \gcd(17, 5) & 17 = 3 \cdot 5 + 2 \qquad \therefore 2 = 17 - 3 \cdot 5 \\ \gcd(5, 2) & 5 = 2 \cdot 2 + 1 \qquad \therefore 1 = 5 - 2 \cdot 2 \end{array}$$

   Now go backwards

$$\begin{aligned} 1 &= 5 - 2 \cdot \underline{2} \\ &= 5 - 2 \cdot (17 - 3 \cdot 5) \\ &= 7 \cdot 5 - 2 \cdot 17 \end{aligned}$$

   So take $x = 7$, i.e. $5^{-1} = 7 \bmod 17$

3. Find integers x and y such that $37x + 29y = 1$.

   First run the Euclidean algorithm to find $\gcd(37, 29)$, keeping track of the steps. We know that the final answer will be 1.

$$\begin{array}{ll} \gcd(29, 37) & 37 = 1 \cdot 29 + 8 \qquad \therefore 8 = 37 - 1 \cdot 29 \\ \gcd(29, 8) & 29 = 3 \cdot 8 + 5 \qquad \therefore 5 = 29 - 3 \cdot 8 \\ \gcd(8, 5) & 8 = 1 \cdot 5 + 3 \qquad \therefore 3 = 8 - 1 \cdot 5 \\ \gcd(5, 3) & 5 = 1 \cdot 3 + 2 \qquad \therefore 2 = 5 - 1 \cdot 3 \\ \gcd(3, 2) & 3 = 1 \cdot 2 + 1 \qquad \therefore 1 = 3 - 1 \cdot 2 \end{array}$$

   Now go backwards

$$\begin{aligned} 1 &= 3 - 1 \cdot \underline{2} \\ &= 3 - 1 \cdot (5 - 1 \cdot 3) \\ &= 2(8 - 1 \cdot 5) - 5 \\ &= 2 \cdot 8 - 3(29 - 3 \cdot 8) \\ &= -3 \cdot 29 + 11(37 - 1 \cdot 29) \\ &= 11 \cdot 37 - 14 \cdot 29 \end{aligned} \qquad \begin{aligned} &= 2 \cdot \underline{3} - 5 \\ &= 2 \cdot 8 - 3 \cdot \underline{5} \\ &= -3 \cdot 29 + 11 \cdot \underline{8} \end{aligned}$$

So $37^{-1} \bmod 29 = 11$ and $29^{-1} = -14 = 23 \bmod 37$.

Exercises 2

1. Find the following inverses. Your answer should be an integer between 0 and $n-1$.
   (a) $29^{-1} \bmod 39$
   (b) $17^{-1} \bmod 39$
   (c) $23^{-1} \bmod 59$
   (d) $45^{-1} \bmod 59$
   (e) $5^{-1} \bmod 59$
   (f) $(-1)^{-1} \bmod 59$

4 Powers in $\mathbb{F}_p$

We may use powers in $\mathbb{F}_p$, $a^b \bmod p$. In particular the corresponding Theorem for multiplication in $\mathbb{F}_p$ (Theorem 9) gives the following

Theorem 20 *For any integers a, b and n, with $n > 1$*

$$a^b \equiv (a \bmod n)^b \pmod{n}$$

This means that we may take mod as we are calculating powers, keeping the intermediate results within reason (less than n).
The most obvious way to calculate powers $a^b \bmod n$ is to multiply a together n times. This takes $O(x)$ operations, and may be succinctly implemented by the following recursive routine.

```
int stdpower(int a, int b, int n) { /*Finds a^b mod n*/
    if(b = 0) return 1;
    else return (a * stdpower(a, b − 1, n)) % n;
}
```

Example 21 *Find* $4^4 \pmod 5$.

$$4 \times 4 \times 4 \times 4 \equiv (16 \bmod 5) \times 4 \times 4 \equiv 1 \times 4 \times 4 \equiv 1 \pmod 5$$

However there is a better way:

```
int fastpower(int a, int b, int n) { /*Finds a^b mod n*/
    if b = 0 return 1;
    else if(b is even) {
        c = fastpower(a, b/2, n);
        return (c*c) % n;
    }
    else return (a * fastpower(a, b − 1, n)) % n;
}
```

This routine effectively looks at the binary representation of b, starting with 1, it squares if that bit is 0 and multiplies by a and then squares if that bit is 1. Thus for each bit of b there are one or two operations, so the running time is (roughly) the the number of bits of n, or $O(\log n)$.

Example 22

1. Run through `fastpower` to find $4^4 \pmod 5$.

   Note that 4 is 100 in binary.

level	power	b	action	return
1	4	100	square	1
2	2	10	square	1 ($\equiv 16 \bmod 5$)
3	1	1	$\times a$	4
4	0	0		1

2. Run through `fastpower` to find $2^5 \pmod 5$.

   Note that 5 is 101 in binary.

level	power	b	action	return
1	5	101	$\times a$	2
2	4	100	square	1
3	2	10	square	4
4	1	1	$\times a$	2
5	0	0		1

3. Run through `fastpower` to find $3^{16} \pmod 7$.

   Note that 16 is 10000 in binary.

level	power	b	action	return
1	16	10000	square	4
2	8	1000	square	2
3	4	100	square	4
4	2	10	square	2
5	1	1	$\times a$	3
6	0	0		1

   6 steps as opposed to the 16 of `stdpower`.

Note that the larger b the better the saving of `fastpower` over `stdpower`
We note that the cancellation theorem for products means that the usual power rules apply.

Theorem 23 *Given integers a, x, y and n, with $n > 1$, then*

$$a^x a^y \equiv a^{x+y} \pmod n \quad \textit{and} \quad a^x a^{-y} \equiv a^{x-y} \pmod n.$$

In particular, $(a^x)^{-1} \equiv a^{-x} \pmod n$

Finally we end this section with a result due to Fermat involving powers over prime fields which is useful.

Theorem 24 (Fermats Little Theorem) *Let p, be any prime and a an integer such that $p \nmid a$, then*

$$a^{p-1} \equiv 1 \pmod{p}$$

SWP

Note that this theorem tells us that so long as $p \nmid a$, $a^{-1} \equiv a^{p-2} \pmod{p}$, giving us an alternative method of finding a^{-1}. In addition it tells us that $a^p \equiv a \pmod{p}$.

Exercises 3

Find the following powers, in each case your answer should be an integer between 1 and n.

1. $3^9 \pmod{13}$
2. $3^6 \pmod{13}$
3. $3^{11} \pmod{13}$
4. $3^{12} \pmod{13}$