MTH314: Discrete Mathematics for Engineers

Lecture 7: Elementary Number Theory

Dr Ewa Infeld

Ryerson University

Prime Numbers

Definition

A number $p \in \mathbb{N}$ is prime if and only if its set of divisors is $D_p = \{\pm 1, \pm p\}$.

- 1 is not a prime. (This is something we need to make other definitions consistent.)
- Let $P(n)$: n is prime. Then the truth set S of $P(n)$ is

$$S = \{n \in \mathbb{N} : \; P(n)\}$$

$$= \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, ...\}$$

- There are infinitely many primes.

Prime Numbers

Theorem

Every natural number $n > 2$ that is not a prime is divisible by at least two primes.

Proof: we will prove this by strong induction. Let:

$$P(n): \; n \text{ is prime or divisible by at least two primes.}$$

We will show that $P(n), \; \forall n \geq 2$. Base case: $P(2)$ is true, since 2 is prime.

Inductive step: we need to show that

$$\forall n > 2, \; [P(2) \wedge P(3) \wedge \cdots \wedge P(n) \rightarrow P(n+1)]$$

Prime Numbers

We need to show that:

$$\forall n > 2,\ [P(2) \wedge P(3) \wedge \cdots \wedge P(n) \to P(n+1)]\,.$$

So fix $k \geq 2$ and assume $P(2), P(3), \ldots, P(k)$ are all true. If $k+1$ is prime, $P(k+1)$ is true and we are done. Otherwise, by definition, it has divisors $a, b < k$ such that $k = a \cdot b$. By the inductive hypothesis both a and b are either primes or divisible by primes and therefore so is k. □

Prime Numbers

We need to show that:

$$\forall n > 2, \ [P(2) \wedge P(3) \wedge \cdots \wedge P(n) \rightarrow P(n+1)] \, .$$

So fix $k \geq 2$ and assume $P(2), P(3), \ldots, P(k)$ are all true. If $k+1$ is prime, $P(k+1)$ is true and we are done. Otherwise, by definition, it has divisors $a, b < k$ such that $k = a \cdot b$. By the inductive hypothesis both a and b are either primes or divisible by primes and therefore so is k. □

A natural number $n > 2$ that is not prime is called composite.

There are infintitely many prime numbers

Theorem

There are infinitely many prime numbers.

Proof: suppose for contradiction that there exists a finite set $P = \{p_1, p_2, \dots, p_k\}$ of all prime numbers. Than any number that is larger than all of those is composite and therefore a product of at least two primes in the set P.

Consider:

$$p = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_k + 1$$

This number is not divisible by any p_i, and therefore has to be prime. □

Sieve of Eratosthenes

To test if a number is prime:

- Check if a number is divisible by small numbers.
- If not, cross out all multiples of those numbers too.
- For any number n, only need to go up to $\sqrt{n}$.

Let's check if 107 is prime.

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68
69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85
86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102
103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119
120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136

Sieve of Eratosthenes

To test if a number is prime:

- Check if a number is divisible by small numbers.
- If not, cross out all multiples of those numbers too.
- For any number n, only need to go up to $\sqrt{n}$.

Let's check if 107 is prime. 2

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68
69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85
86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102
103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119
120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136

Sieve of Eratosthenes

To test if a number is prime:

- Check if a number is divisible by small numbers.
- If not, cross out all multiples of those numbers too.
- For any number n, only need to go up to $\sqrt{n}$.

Let's check if 107 is prime. 2

	~~2~~	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11	~~12~~	13	~~14~~	15	~~16~~	17
~~18~~	19	~~20~~	21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~	31	~~32~~	33	~~34~~
35	~~36~~	37	~~38~~	39	~~40~~	41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~	51
~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~	61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~
69	~~70~~	71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~	81	~~82~~	83	~~84~~	85
~~86~~	87	~~88~~	89	~~90~~	91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~	101	~~102~~
103	~~104~~	105	~~106~~	107	~~108~~	109	~~110~~	111	~~112~~	113	~~114~~	115	~~116~~	117	~~118~~	119
~~120~~	121	~~122~~	123	~~124~~	125	~~126~~	127	~~128~~	129	~~130~~	131	~~132~~	133	~~134~~	135	~~136~~

Sieve of Eratosthenes

To test if a number is prime:

- Check if a number is divisible by small numbers.
- If not, cross out all multiples of those numbers too.
- For any number n, only need to go up to $\sqrt{n}$.

Let's check if 107 is prime. 2, 3

	~~2~~	~~3~~	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~	17
~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~
35	~~36~~	37	~~38~~	~~39~~	~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~	~~51~~
~~52~~	53	~~54~~	55	~~56~~	~~57~~	~~58~~	59	~~60~~	61	~~62~~	~~63~~	~~64~~	65	~~66~~	67	~~68~~
~~69~~	~~70~~	71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~	~~81~~	~~82~~	83	~~84~~	85
~~86~~	~~87~~	~~88~~	89	~~90~~	91	~~92~~	~~93~~	~~94~~	95	~~96~~	97	~~98~~	~~99~~	~~100~~	101	~~102~~
103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~	~~111~~	~~112~~	113	~~114~~	115	~~116~~	~~117~~	~~118~~	119
~~120~~	121	~~122~~	~~123~~	~~124~~	125	~~126~~	127	~~128~~	~~129~~	~~130~~	131	~~132~~	133	~~134~~	~~135~~	~~136~~

Sieve of Eratosthenes

To test if a number is prime:

- Check if a number is divisible by small numbers.
- If not, cross out all multiples of those numbers too.
- For any number n, only need to go up to $\sqrt{n}$.

Let's check if 107 is prime. 2,3,5

	~~2~~	~~3~~	~~4~~	~~5~~	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~	17
~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~
~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~	~~51~~
~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~	61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~
~~69~~	~~70~~	71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~	~~81~~	~~82~~	83	~~84~~	~~85~~
~~86~~	~~87~~	~~88~~	89	~~90~~	91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~	101	~~102~~
103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~	~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	119
~~120~~	121	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~	131	~~132~~	133	~~134~~	~~135~~	~~136~~

Sieve of Eratosthenes

To test if a number is prime:

- Check if a number is divisible by small numbers.
- If not, cross out all multiples of those numbers too.
- For any number n, only need to go up to $\sqrt{n}$.

Let's check if 107 is prime. 2,3,5,7,11

	~~2~~	~~3~~	~~4~~	~~5~~	~~6~~	~~7~~	~~8~~	~~9~~	~~10~~	~~11~~	~~12~~	13	~~14~~	~~15~~	~~16~~	17
~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~
~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~	~~51~~
~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~	61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~
~~69~~	~~70~~	71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~	~~81~~	~~82~~	83	~~84~~	~~85~~
~~86~~	~~87~~	~~88~~	89	~~90~~	~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~	101	~~102~~
103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~	~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~
~~120~~	~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~	131	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~

So all prime numbers up to 136 are...

So all prime numbers up to 136 are...

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

Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic)

Every integer greater than 1 has a unique representation as a product of primes. (Written in increasing order.)

Example: 112

Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic)

Every integer greater than 1 has a unique representation as a product of primes. (Written in increasing order.)

Examples:
$112 = 2^5 \cdot 7$

Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic)

Every integer greater than 1 has a unique representation as a product of primes. (Written in increasing order.)

Examples:
$112 = 2^5 \cdot 7$
$100 = 2^2 \cdot 5^2$

Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic)

Every integer greater than 1 has a unique representation as a product of primes. (Written in increasing order.)

Examples:
$112 = 2^4 \cdot 7$
$100 = 2^2 \cdot 5^2$

Find the prime power decomposition of the following numbers:

- 2040
- 551
- 1144
- 32805

Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic)

Every integer greater than 1 has a unique representation as a product of primes. (Written in increasing order.)

Examples:
$112 = 2^5 \cdot 7$
$100 = 2^2 \cdot 5^2$

Find the prime power decomposition of the following numbers:

- 2040 $2^3 \cdot 3 \cdot 5 \cdot 17$
- 551
- 1144
- 32805

Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic)

Every integer greater than 1 has a unique representation as a product of primes. (Written in increasing order.)

Examples:
$112 = 2^5 \cdot 7$
$100 = 2^2 \cdot 5^2$

Find the prime power decomposition of the following numbers:

- 2040 $2^3 \cdot 3 \cdot 5 \cdot 17$
- 551 $19 \cdot 29$
- 1144
- 32805

Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic)

Every integer greater than 1 has a unique representation as a product of primes. (Written in increasing order.)

Examples:
$112 = 2^4 \cdot 7$
$100 = 2^2 \cdot 5^2$

Find the prime power decomposition of the following numbers:

- 2040 $2^3 \cdot 3 \cdot 5 \cdot 17$
- 551 $19 \cdot 29$
- 1144 $2^3 \cdot 11 \cdot 13$
- 32805

Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic)

Every integer greater than 1 has a unique representation as a product of primes. (Written in increasing order.)

Examples:
$112 = 2^5 \cdot 7$
$100 = 2^2 \cdot 5^2$

Find the prime power decomposition of the following numbers:

■ 2040	$2^3 \cdot 3 \cdot 5 \cdot 17$
■ 551	$19 \cdot 29$
■ 1144	$2^3 \cdot 11 \cdot 13$
■ 32805	$3^8 \cdot 5$

Prime factorization

Theorem

If p is prime and $p|a \cdot b$ then p divides at least one among a, b.

Proof: Suppose $p \not| b$ (as otherwise we are done). Then $GCD(p, b) = 1$ (because p is prime), and hence $p|a$. □

Fun Facts

Theorem

If p is prime and $p|a \cdot b$ then p divides at least one among a, b.

Proof: Suppose $p \not| b$ (as otherwise we are done). Then $GCD(p, b) = 1$ (because p is prime), and hence $p|a$. □

Corollary

If p is prime and $p|(a_1 \cdot a_2 \cdot \ldots \cdot a_n)$ then p divides at least one of a_i .

Sketch of proof: Induction on n, with inductive step as above.

Fun Facts

Theorem

If p is prime and $p | a \cdot b$ then p divides at least one among a, b.

Proof: Suppose $p \not| b$ (as otherwise we are done). Then $GCD(p, b) = 1$ (because p is prime), and hence $p | a$. □

Corollary

If p is prime and $p | (a_1 \cdot a_2 \cdot \ldots \cdot a_n)$ then p divides at least one of a_i .

Sketch of proof: Induction on n, with inductive step as above.

Lemma

If for two primes p, q we have $p | q$, then $p = q$.

Efficient factorization

We don't have good algorithms for factorization of a given large number n (*good* in this case means polynomial in $\log(n)$.)

There's an efficient algorithm to do it with a quantum computer (Shor's algorithm.)

Commonly used encryption systems rely on the fact that factorization is hard. The moment someone invents a good (non-quantum) factorization algorithm or builds a quantum computer all that encryption will be broken.

Prime power decomposition and GCDs

Exercise: use the prime power decomposition you've obtained before to find:

$GCD(2040, 1144) =$

$GCD(2040, 32805) =$

Think of any 3 digit integer, and call it x. Suppose the digits are A, B and C so

$$x = ABC$$

Reorder its digits anyway you like and call the result y, this could be for example CBA.
Compute $|x - y|$, it's going to be another three digit integer. If it's 2 or 1 digit we'll just add 0's at the front. Now, if you tell me any two digits of $|x - y|$, I can tell you what the third digit is. How?

Think of any 3 digit integer, and call it x. Suppose the digits are A, B and C so

$$x = ABC$$

Reorder its digits anyway you like and call the result y, this could be for example CBA.
Compute $|x - y|$, it's going to be another three digit integer. If it's 2 or 1 digit we'll just add 0's at the front. Now, if you tell me any two digits of $|x - y|$, I can tell you what the third digit is. How?

Example: say, $x = 724$ and $y = 427$. Then $|x - y| = 297$. If you gave me any two of $2, 9, 7$ I would be able to guess the third.

Congruences

For two integers a, b with $b > 0$, if

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

for some integers q, r we say that:

$$a \equiv r \ (mod \ \ b).$$

"a is equivalent to r modulo b" or "a is congruent to r mod b."

Definition (congruence)

For all integers a, r and a positive integer b, we say that a is congruent to r modulo b iff

$$b|(a - r).$$

Congruences

Definition (congruence)

For all integers a, r and a positive integer b, we say that a is congruent to r modulo b iff

$$b|(a-r).$$

Example:

$$17 \equiv 2 \ (mod\ 5)$$

Because the remainder of 17 when dividing by 5 is 2. Equivalently, because $17 - 2 = 15$, and 15 is divisible by 5.

Congruences

Definition (congruence)

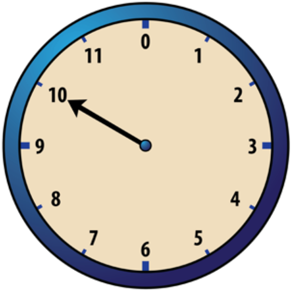
For all integers a, r and a positive integer b, we say that a is congruent to r modulo b iff

$$b|(a-r).$$

Example:

$$17 \equiv 2 \ (mod \ 5)$$

Because the remainder of 17 when dividing by 5 is 2. Equivalently, because $17 - 2 = 15$, and 15 is divisible by 5.



This is sometimes called “clockwork arithmetic” because on a clock we tell hours modulo 12. It takes 12 hours to make a full circle and get back where we started.

Adding and multiplying

Notice that if $a \equiv a' \ (mod \ c)$ and $b \equiv b' \ (mod \ c)$, then:

$$a + b \equiv a' + b' \ (mod \ c)$$

It might be that $a' + b' \geq c$, and can be simplified.

Adding and multiplying

Notice that if $a \equiv a' \ (mod\ \ c)$ and $b \equiv b' \ (mod\ \ c)$, then:

$$a + b \equiv a' + b' \ (mod\ \ c)$$

It might be that $a' + b' \geq c$, and can be simplified.

Examples:

- $79 + 92 \equiv \qquad\qquad (mod\ 7)$
  $171 \equiv \quad (mod\ 7)$
- $139 \equiv \quad (mod\ 7)$
- $133 + 21 \equiv \qquad\qquad (mod\ 19)$
  $154 \equiv \quad (mod\ 19)$

Adding and multiplying

Notice that if $a \equiv a' \pmod{c}$ and $b \equiv b' \pmod{c}$, then:

$$a + b \equiv a' + b' \pmod{c}$$

It might be that $a' + b' \geq c$, and can be simplified.

Examples:

- $79 + 92 \equiv 2 + 1 \pmod{7}$
  $171 \equiv 3 \pmod{7}$
- $139 \equiv \quad \pmod{7}$
- $133 + 21 \equiv \qquad \pmod{19}$
  $154 \equiv \quad \pmod{19}$

Adding and multiplying

Notice that if $a \equiv a' \ (mod \ \ c)$ and $b \equiv b' \ (mod \ \ c)$, then:

$$a + b \equiv a' + b' \ (mod \ \ c)$$

It might be that $a' + b' \geq c$, and can be simplified.

Examples:

- $79 + 92 \equiv 2 + 1 \ (mod \ 7)$
  $171 \equiv 3 \ (mod \ 7)$

- $139 \equiv \quad (mod \ 7)$
  $140 - 1 \equiv 0 - 1 \ (mod \ 7) \equiv 6 \ (mod \ 7)$

- $133 + 21 \equiv \qquad\quad (mod \ 19)$
  $154 \equiv \quad (mod \ 18)$

Adding and multiplying

Notice that if $a \equiv a' \ (mod \ \ c)$ and $b \equiv b' \ (mod \ \ c)$, then:

$$a + b \equiv a' + b' \ (mod \ \ c)$$

It might be that $a' + b' \geq c$, and can be simplified.

Examples:

- $79 + 92 \equiv 2 + 1 \ (mod \ 7)$
  $171 \equiv 3 \ (mod \ 7)$

- $139 \equiv 6 \ (mod \ 7)$
  $140 - 1 \equiv 0 - 1 \ (mod \ 7) \equiv 6 \ (mod \ 7)$

- $133 + 21 \equiv \qquad (mod \ 19)$
  $154 \equiv \quad (mod \ 19)$

Adding and multiplying

Notice that if $a \equiv a' \pmod{c}$ and $b \equiv b' \pmod{c}$, then:

$$a + b \equiv a' + b' \pmod{c}$$

It might be that $a' + b' \geq c$, and can be simplified.

Examples:

- $79 + 92 \equiv 2 + 1 \pmod{7}$
  $171 \equiv 3 \pmod{7}$

- $139 \equiv 6 \pmod{7}$
  $140 - 1 \equiv 0 - 1 \pmod{7} \equiv 6 \pmod{7}$

- $133 + 21 \equiv 0 + 2 \pmod{19}$
  $154 \equiv 2 \pmod{19}$

Adding and multiplying

If we can add congruences, then we can multiply them too (since multiplication is really adding several copies of the same thing.) So if $a \equiv a' \ (mod \ c)$ and $b \equiv b' \ (mod \ c)$, then:

$$a \cdot b \equiv a' \cdot b' \ (mod \ c)$$

It might be that $a' \cdot b' \geq c$, and can be simplified.

Examples:

- $79 \cdot 92 \equiv \qquad (mod \ 7)$
  $7268 \equiv \quad (mod \ 7)$
- $133 = \qquad\qquad (mod \ 6)$

Adding and multiplying

If we can add congruences, then we can multiply them too (since multiplication is really adding several copies of the same thing.) So if $a \equiv a' \ (mod \ c)$ and $b \equiv b' \ (mod \ c)$, then:

$$a \cdot b \equiv a' \cdot b' \ (mod \ c)$$

It might be that $a' \cdot b' \geq c$, and can be simplified.

Examples:

- $79 \cdot 92 \equiv 2 \cdot 1 \ (mod \ 7)$
  $7268 \equiv 2 \ (mod \ 7)$
- $133 = \qquad\qquad (mod \ 6)$

Adding and multiplying

If we can add congruences, then we can multiply them too (since multiplication is really adding several copies of the same thing.) So if $a \equiv a' \ (mod \ c)$ and $b \equiv b' \ (mod \ c)$, then:

$$a \cdot b \equiv a' \cdot b' \ (mod \ c)$$

It might be that $a' \cdot b' \geq c$, and can be simplified.

Examples:

- $79 \cdot 92 \equiv 2 \cdot 1 \ (mod \ 7)$
  $7268 \equiv 2 \ (mod \ 7)$
- $133 = 7 \cdot 19 \equiv 1 \ (mod \ 6)$
  Verify: $133 = 132 + 1 = 22 \cdot 2 + 1$ ✓.

Adding and multiplying

If we can add congruences, then we can multiply them too (since multiplication is really adding several copies of the same thing.) So if $a \equiv a' \ (mod \ c)$ and $b \equiv b' \ (mod \ c)$, then:

$$a \cdot b \equiv a' \cdot b' \ (mod \ c)$$

It might be that $a' \cdot b' \geq c$, and can be simplified.

Proof:

Adding and multiplying

If we can add congruences, then we can multiply them too (since multiplication is really adding several copies of the same thing.) So if $a \equiv a' \ (mod \ c)$ and $b \equiv b' \ (mod \ c)$, then:

$$a \cdot b \equiv a' \cdot b' \ (mod \ c)$$

It might be that $a' \cdot b' \geq c$, and can be simplified.

Proof:

Adding and multiplying

If we can add congruences, then we can multiply them too (since multiplication is really adding several copies of the same thing.) So if $a \equiv a' \ (mod \ c)$ and $b \equiv b' \ (mod \ c)$, then:

$$a \cdot b \equiv a' \cdot b' \ (mod \ c)$$

It might be that $a' \cdot b' \geq c$, and can be simplified.

Proof: Suppose that $a = q_1 \cdot c + a'$ and $b = q_2 \cdot c + b'$. Then:

$$a \cdot b = q_1 \cdot q_2 \cdot c^2 + q_1 \cdot c \cdot b' + q_2 \cdot c \cdot a' + a' \cdot b'.$$

So the remainder of $a \cdot b$ when dividing by c is the same as the remainder of $a' \cdot b'$, since all the other summands are divisible by c.

□

Adding and multiplying

If we can multiply, then we can use powers too.

So if $a \equiv a' \ (mod \ c)$, then:

$$a^n \equiv (a')^n (mod \ c)$$

It might be that $(a')^n \geq c$, and can be simplified.

Example: find the remainder when 3^{2005} is divided by 5.

Adding and multiplying

If we can multiply, then we can use powers too.

So if $a \equiv a' \ (mod \ c)$, then:

$$a^n \equiv (a')^n (mod \ c)$$

It might be that $(a')^n \geq c$, and can be simplified.

Example: find the remainder when 3^{2005} is divided by 5.

$3 \equiv 3 \ (mod \ 5)$
$3^2 = 9 \equiv 4 \ (mod \ 5)$
$3^3 = 27 \equiv 2 \ (mod \ 5)$
$3^4 \equiv 2 \cdot 3 \ (mod \ 5) \equiv 1 \ (mod \ 5)$

Adding and multiplying

If we can multiply, then we can use powers too.

So if $a \equiv a' \ (mod \ c)$, then:

$$a^n \equiv (a')^n (mod \ c)$$

It might be that $(a')^n \geq c$, and can be simplified.

Example: find the remainder when 3^{2005} is divided by 5.

$3 \equiv 3 \ (mod \ 5)$
$3^2 = 9 \equiv 4 \ (mod \ 5)$
$3^3 = 27 \equiv 2 \ (mod \ 5)$
$3^4 \equiv 2 \cdot 3 \ (mod \ 5) \equiv 1 \ (mod \ 5)$ (!!!)

We have $2005 = 2004 + 1$, so $3^{2005} = 3^{2004} \cdot 3$

Adding and multiplying

If we can multiply, then we can use powers too.

So if $a \equiv a' \ (mod \ c)$, then:

$$a^n \equiv (a')^n (mod \ c)$$

It might be that $(a')^n \geq c$, and can be simplified.

Example: find the remainder when 3^{2005} is divided by 5.

$3 \equiv 3 \ (mod \ 5)$
$3^2 = 9 \equiv 4 \ (mod \ 5)$
$3^3 = 27 \equiv 2 \ (mod \ 5)$
$3^4 \equiv 2 \cdot 3 \ (mod \ 5) \equiv 1 \ (mod \ 5)$ (!!!)

We have $2005 = 2004 + 1$, so $3^{2005} = 3^{2004} \cdot 3 = (3^4)^{501} \cdot 3$

Adding and multiplying

If we can multiply, then we can use powers too.

So if $a \equiv a' \ (mod\ c)$, then:

$$a^n \equiv (a')^n (mod\ c)$$

It might be that $(a')^n \geq c$, and can be simplified.

Example: find the remainder when 3^{2005} is divided by 5.

$3 \equiv 3 \ (mod\ 5)$

$3^2 = 9 \equiv 4 \ (mod\ 5)$

$3^3 = 27 \equiv 2 \ (mod\ 5)$

$3^4 \equiv 2 \cdot 3 \ (mod\ 5) \equiv 1 \ (mod\ 5)$

$3^{2005} \equiv \qquad (mod\ 5)$

$3^{2005} \equiv \qquad (mod\ 5)$

$3^{2005} \equiv \qquad (mod\ 5)$

$3^{2005} \equiv \quad (mod\ 5)$

We have $2005 = 2004 + 1$, so $3^{2005} = 3^{2004} \cdot 3 = (3^4)^{501} \cdot 3$

Adding and multiplying

If we can multiply, then we can use powers too.

So if $a \equiv a' \ (mod\ c)$, then:

$$a^n \equiv (a')^n (mod\ c)$$

It might be that $(a')^n \geq c$, and can be simplified.

Example: find the remainder when 3^{2005} is divided by 5.

$3 \equiv 3 \ (mod\ 5)$
$3^2 = 9 \equiv 4 \ (mod\ 5)$
$3^3 = 27 \equiv 2 \ (mod\ 5)$
$3^4 \equiv 2 \cdot 3 \ (mod\ 5) \equiv 1 \ (mod\ 5)$

$3^{2005} \equiv (3^4)^{501} \cdot 3 \ (mod\ 5)$
$3^{2005} \equiv \qquad (mod\ 5)$
$3^{2005} \equiv \qquad (mod\ 5)$
$3^{2005} \equiv \quad (mod\ 5)$

We have $2005 = 2004 + 1$, so $3^{2005} = 3^{2004} \cdot 3 = (3^4)^{501} \cdot 3$

Adding and multiplying

If we can multiply, then we can use powers too.

So if $a \equiv a' \ (mod \ c)$, then:

$$a^n \equiv (a')^n (mod \ c)$$

It might be that $(a')^n \geq c$, and can be simplified.

Example: find the remainder when 3^{2005} is divided by 5.

$3 \equiv 3 \ (mod \ 5)$
$3^2 = 9 \equiv 4 \ (mod \ 5)$
$3^3 = 27 \equiv 2 \ (mod \ 5)$
$3^4 \equiv 2 \cdot 3 \ (mod \ 5) \equiv 1 \ (mod \ 5)$

$3^{2005} \equiv (3^4)^{501} \cdot 3 \ (mod \ 5)$
$3^{2005} \equiv (1)^{501} \cdot 3 \ (mod \ 5)$
$3^{2005} \equiv \quad (mod \ 5)$
$3^{2005} \equiv \quad (mod \ 5)$

We have $2005 = 2004 + 1$, so $3^{2005} = 3^{2004} \cdot 3 = (3^4)^{501} \cdot 3$

Adding and multiplying

If we can multiply, then we can use powers too.

So if $a \equiv a' \ (mod \ c)$, then:

$$a^n \equiv (a')^n (mod \ c)$$

It might be that $(a')^n \geq c$, and can be simplified.

Example: find the remainder when 3^{2005} is divided by 5.

$3 \equiv 3 \ (mod \ 5)$
$3^2 = 9 \equiv 4 \ (mod \ 5)$
$3^3 = 27 \equiv 2 \ (mod \ 5)$
$3^4 \equiv 2 \cdot 3 \ (mod \ 5) \equiv 1 \ (mod \ 5)$

$3^{2005} \equiv (3^4)^{501} \cdot 3 \ (mod \ 5)$
$3^{2005} \equiv (1)^{501} \cdot 3 \ (mod \ 5)$
$3^{2005} \equiv 1 \cdot 3 \ (mod \ 5)$
$3^{2005} \equiv 3 \ (mod \ 5)$

We have $2005 = 2004 + 1$, so $3^{2005} = 3^{2004} \cdot 3 = (3^4)^{501} \cdot 3$

- Find the remainder when 5^{117} is divided by 6.

- Find the remainder when 11^{2897} is divided by 10.

- Find the remainder when 11^{1001} is divided by 100.

- Find the remainder when 5^{117} is divided by 6.
  $5^2 = 25 \equiv 1 \ (mod\ 6)$
  $117 \equiv 1 \ (mod\ 2)$
  $5^{117} = (5^2)^{58} \cdot 5 \equiv 5 \ (mod\ 6)$
- Find the remainder when 11^{2897} is divided by 10.

- Find the remainder when 11^{1001} is divided by 100. .

- Find the remainder when 5^{117} is divided by 6.
  $5^2 = 25 \equiv 1 \ (mod\ 6)$
  $117 \equiv 1 \ (mod\ 2)$
  $5^{117} = (5^2)^{58} \cdot 5 \equiv 5 \ (mod\ 6)$
- Find the remainder when 11^{2897} is divided by 10.
  $11^2 = 121 \equiv 1 \ (mod\ 10)$
  $2897 \equiv 1 \ (mod\ 2)$
  $11^{2897} = (11^2)^n \cdot 11 \equiv 11 \ (mod\ 10)$
- Find the remainder when 11^{1001} is divided by 100.

- Find the remainder when 5^{117} is divided by 6.
  $5^2 = 25 \equiv 1 \ (mod\ 6)$
  $117 \equiv 1 \ (mod\ 2)$
  $5^{117} = (5^2)^{58} \cdot 5 \equiv 5 \ (mod\ 6)$
- Find the remainder when 11^{2897} is divided by 10.
  $11^2 = 121 \equiv 1 \ (mod\ 10)$
  $2897 \equiv 1 \ (mod\ 2)$
  $11^{2897} = (11^2)^n \cdot 11 \equiv 11 \ (mod\ 10)$
- Find the remainder when 11^{1001} is divided by 100.
  $11^2 \equiv 21 \ (mod\ 100)$

- Find the remainder when 5^{117} is divided by 6.
  $5^2 = 25 \equiv 1 \ (mod \ 6)$
  $117 \equiv 1 \ (mod \ 2)$
  $5^{117} = (5^2)^{58} \cdot 5 \equiv 5 \ (mod \ 6)$
- Find the remainder when 11^{2897} is divided by 10.
  $11^2 = 121 \equiv 1 \ (mod \ 10)$
  $2897 \equiv 1 \ (mod \ 2)$
  $11^{2897} = (11^2)^n \cdot 11 \equiv 11 \ (mod \ 10)$
- Find the remainder when 11^{1001} is divided by 100.
  $11^2 \equiv 21 \ (mod \ 100)$
  $11^3 \equiv 21 \cdot 11 \ (mod \ 100) \equiv 31 \ (mod \ 100)$

- Find the remainder when 5^{117} is divided by 6.
  $5^2 = 25 \equiv 1 \ (mod\ 6)$
  $117 \equiv 1 \ (mod\ 2)$
  $5^{117} = (5^2)^{58} \cdot 5 \equiv 5 \ (mod\ 6)$
- Find the remainder when 11^{2897} is divided by 10.
  $11^2 = 121 \equiv 1 \ (mod\ 10)$
  $2897 \equiv 1 \ (mod\ 2)$
  $11^{2897} = (11^2)^n \cdot 11 \equiv 11 \ (mod\ 10)$
- Find the remainder when 11^{1001} is divided by 100.
  $11^2 \equiv 21 \ (mod\ 100)$
  $11^3 \equiv 21 \cdot 11 \ (mod\ 100) \equiv 31 \ (mod\ 100)$
  $11^4 \equiv 31 \cdot 11 \ (mod\ 100) \equiv 41 \ (mod\ 100)$

- Find the remainder when 5^{117} is divided by 6.
  $5^2 = 25 \equiv 1 \ (mod \ 6)$
  $117 \equiv 1 \ (mod \ 2)$
  $5^{117} = (5^2)^5 8 \cdot 5 \equiv 5 \ (mod \ 6)$
- Find the remainder when 11^{2897} is divided by 10.
  $11^2 = 121 \equiv 1 \ (mod \ 10)$
  $2897 \equiv 1 \ (mod \ 2)$
  $11^{2897} = (11^2)^n \cdot 11 \equiv 11 \ (mod \ 10)$
- Find the remainder when 11^{1001} is divided by 100.
  $11^2 \equiv 21 \ (mod \ 100)$
  $11^3 \equiv 21 \cdot 11 \ (mod \ 100) \equiv 31 \ (mod \ 100)$
  $11^4 \equiv 31 \cdot 11 \ (mod \ 100) \equiv 41 \ (mod \ 100)$
  $11^5 \equiv 41 \cdot 11 \ (mod \ 100) \equiv 51 \ (mod \ 100)$
  $\vdots$
  $11^{10} \equiv 91 \cdot 11 \ (mod \ 100) \equiv 1 \ (mod \ 100)$

- Find the remainder when 11^{1001} is divided by 100.
  $11^2 \equiv 21 \ (mod\ 100)$
  $11^3 \equiv 21 \cdot 11 \ (mod\ 100) \equiv 31 \ (mod\ 100)$
  $11^4 \equiv 31 \cdot 11 \ (mod\ 100) \equiv 41 \ (mod\ 100)$
  $11^5 \equiv 41 \cdot 11 \ (mod\ 100) \equiv 51 \ (mod\ 100)$
  $\vdots$
  $11^{10} \equiv 91 \cdot 11 \ (mod\ 100) \equiv 1 \ (mod\ 100)$

$$1001 = 1000 + 1 \equiv 1 \ (mod\ 10)$$

- Find the remainder when 11^{1001} is divided by 100.
  $11^2 \equiv 21 \ (mod\ 100)$
  $11^3 \equiv 21 \cdot 11 \ (mod\ 100) \equiv 31 \ (mod\ 100)$
  $11^4 \equiv 31 \cdot 11 \ (mod\ 100) \equiv 41 \ (mod\ 100)$
  $11^5 \equiv 41 \cdot 11 \ (mod\ 100) \equiv 51 \ (mod\ 100)$
  $\vdots$
  $11^{10} \equiv 91 \cdot 11 \ (mod\ 100) \equiv 1 \ (mod\ 100)$

$$1001 = 1000 + 1 \equiv 1 \ (mod\ 10)$$

$$11^{1001} = (11^{10})^{100} \cdot 11$$

- Find the remainder when 11^{1001} is divided by 100.
  $11^2 \equiv 21 \ (mod\ 100)$
  $11^3 \equiv 21 \cdot 11 \ (mod\ 100) \equiv 31 \ (mod\ 100)$
  $11^4 \equiv 31 \cdot 11 \ (mod\ 100) \equiv 41 \ (mod\ 100)$
  $11^5 \equiv 41 \cdot 11 \ (mod\ 100) \equiv 51 \ (mod\ 100)$
  $\vdots$
  $11^{10} \equiv 91 \cdot 11 \ (mod\ 100) \equiv 1 \ (mod\ 100)$

$$1001 = 1000 + 1 \equiv 1 \ (mod\ 10)$$

$$11^{1001} = (11^{10})^{100} \cdot 11$$

$$\equiv 11 \ (mod\ 100)$$

More about GCD

Linear congruences

Definition

For all integers a, b, and positive integer m, and for variable x, we call the equation

$$a \cdot x \equiv b\ (mod\ \ m)$$

a linear congruence in x.

Linear congruences

Definition

For all integers a, b, and positive integer m, and for variable x, we call the equation

$$a \cdot x \equiv b \ (mod \ \ m)$$

a linear congruence in x.

Example: $3x \equiv -2 \ (mod \ 10)$ is a linear congruence in x.

To solve it, we need to find all congruences $x \ (mod \ 10)$ such that $3x \equiv 8 \ (mod \ 10)$.

Linear congruences

Definition

For all integers a, b, and positive integer m, and for variable x, we call the equation

$$a \cdot x \equiv b \ (mod \ \ m)$$

a linear congruence in x.

Example: $3x \equiv -2 \ (mod \ 10)$ is a linear congruence in x.

To solve it, we need to find all congruences $x \ (mod \ 10)$ such that $3x \equiv 8 \ (mod \ 10)$. With 10 that's not too bad, we only have 10 to check:

$3 \cdot 0 \equiv 0 \ (mod \ 10)$
$3 \cdot 1 \equiv 3 \ (mod \ 10)$
$3 \cdot 2 \equiv 6 \ (mod \ 10)$
$3 \cdot 3 \equiv 9 \ (mod \ 10)$
$3 \cdot 4 \equiv 2 \ (mod \ 10)$
$3 \cdot 5 \equiv 5 \ (mod \ 10)$
$3 \cdot 6 \equiv 8 \ (mod \ 10)$
$3 \cdot 7 \equiv 1 \ (mod \ 10)$
$3 \cdot 8 \equiv 4 \ (mod \ 10)$
$3 \cdot 9 \equiv 7 \ (mod \ 10)$

Linear congruences

Definition

For all integers a, b, and positive integer m, and for variable x, we call the equation

$$a \cdot x \equiv b \ (mod \ \ m)$$

a linear congruence in x.

Example: $3x \equiv -2 \ (mod \ 10)$ is a linear congruence in x.

To solve it, we need to find all congruences $x \ (mod \ 10)$ such that $3x \equiv 8 \ (mod \ 10)$. With 10 that's not too bad, we only have 10 to check:

$3 \cdot 0 \equiv 0 \ (mod \ 10)$
$3 \cdot 1 \equiv 3 \ (mod \ 10)$
$3 \cdot 2 \equiv 6 \ (mod \ 10)$
$3 \cdot 3 \equiv 9 \ (mod \ 10)$
$3 \cdot 4 \equiv 2 \ (mod \ 10)$
$3 \cdot 5 \equiv 5 \ (mod \ 10)$
$3 \cdot 6 \equiv 8 \ (mod \ 10)$
$3 \cdot 7 \equiv 1 \ (mod \ 10)$
$3 \cdot 8 \equiv 4 \ (mod \ 10)$
$3 \cdot 9 \equiv 7 \ (mod \ 10)$

Linear congruences

Definition

For all integers a, b, and positive integer m, and for variable x, we call the equation

$$a \cdot x \equiv b \ (mod \ \ m)$$

a linear congruence in x.

Theorem

The linear congruence $a \cdot x \equiv b \ (mod \ \ m)$ has a solution if and only if the LDE $a \cdot x + m \cdot y = b$ has a solution.

Linear congruences

Definition

For all integers a, b, and positive integer m, and for variable x, we call the equation

$$a \cdot x \equiv b \ (mod \ \ m)$$

a linear congruence in x.

Theorem (Linear congruence theorem)

The linear congruence $a \cdot x \equiv b \ (mod \ \ m)$ has a solution if and only if the LDE $a \cdot x + m \cdot y = b$ has a solution.

In other words, the linear congruence $a \cdot x \equiv b \ (mod \ \ m)$ has a solution if and only if $GCD(a, m)|b$. Then it has $GCD(a, m)$ solutions.

Theorem (Linear congruence theorem)

If the linear congruence $a \cdot x \equiv b \ (mod \ m)$ has a solution x_0, then all solutions are all integers x with:

$$x \equiv x_0 \ (mod \ \frac{m}{GCD(a,m)}).$$

Example: $5 \cdot x \equiv 5 \ (mod \ 10)$ has solutions because:

$$GCD(5,10) = 5 \mid 5 \checkmark$$

$x_0 = 1$ is a solution. All other congruence class solutions are such that

$$x \equiv 1 \ (mod \ \frac{10}{5})$$

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

Example

Solve the linear congruence in x,

$$18 \cdot x \equiv 10 \ (mod\ 14).$$

It's solving the LDE $18 \cdot x + 14 \cdot y = 10$:

1. Check that $GCD(18, 14)$ divides 10.
2. If it does, find one solution x_0.
3. There are $GCD(18, 14)$ solutions are of the form $x \equiv x_0 \ (mod \frac{14}{GCD(18,14)})$

Example

Solve the linear congruence in x,

$$18 \cdot x \equiv 10 \ (mod\ 14).$$

It's solving the LDE $18 \cdot x + 14 \cdot y = 10$:

1. Check that $GCD(18, 14)$ divides 10.
2. If it does, find one solution x_0.
3. There are $GCD(18, 14)$ solutions are of the form $x \equiv x_0 \ (mod \frac{14}{GCD(18,14)})$

1. Yes, $GCD(18, 14) = 2$ and it divides 10.
2. We find one solution from the Euclidean Algorithm.
3. There are 2 solutions, x_0 and $x_0 + \frac{14}{2} = x_0 + 7$.

Example

Solve the linear congruence in x,

$$18 \cdot x \equiv 10 \ (mod\ 14).$$

It's solving the LDE $18 \cdot x + 14 \cdot y = 10$:

$18 = 14 + 4$
$14 = 3 \cdot 4 + 2$

$2 = 14 - 3 \cdot 4$
$2 = 14 - 3(18 - 14) = 4 \cdot 14 - 3 \cdot 18$

$$4 \cdot 14 - 3 \cdot 18 = 2$$

$$20 \cdot 14 - 15 \cdot 18 = 10$$

So $x_0 = -15, \ y_0 = 20$ is a solution of the LDE.

$$-15 \equiv -1 \ (mod\ 14)$$

Example

Solve the linear congruence in x,

$$18 \cdot x \equiv 10 \ (mod\ 14).$$

It's solving the LDE $18 \cdot x + 14 \cdot y = 10$:

$x_0 = -15, \ y_0 = 20$ is a solution of the LDE.

$$-15 \equiv -1 \ (mod\ 14)$$

Verify: $18 \cdot (-1) = -18 \equiv 10 \ (mod\ 14)$. So the complete set of congruence class solutions of the congruence equation is:

$$x_0 = -1 \text{ and } x_1 = -1 + 7 = 6.$$

Example

Solve the linear congruence in x,

$$18 \cdot x \equiv 10 \ (mod\ 14).$$

It's solving the LDE $18 \cdot x + 14 \cdot y = 10$:

$x_0 = -15,\ y_0 = 20$ is a solution of the LDE.

$$-15 \equiv -1 \ (mod\ 14)$$

Verify: $18 \cdot (-1) = -18 \equiv 10 \ (mod\ 14)$. So the complete set of congruence class solutions of the congruence equation is:

$$x_0 = -1 \text{ and } x_1 = -1 + 7 = 6.$$

Or we could just write $x \equiv 6 \ (mod\ 7)$.

So the solutions to the worksheet are so far:

a) $2 \cdot x \equiv 8 \ (mod \ 10)$

$$x \equiv 4 \ (mod \ 10) \text{ or } x \equiv 9 \ (mod \ 10)$$

Or better still:

$$x \equiv 4 \ (mod \ 5).$$

b) $5 \cdot x \equiv 5 \ (mod \ 10)$

c) $18 \cdot x \equiv 10 \ (mod \ 14)$

So the solutions to the worksheet are so far:

a) $2 \cdot x \equiv 8 \ (mod\ 10)$

$$x \equiv 4 \ (mod\ 10) \text{ or } x \equiv 9 \ (mod\ 10)$$

Or better still:

$$x \equiv 4 \ (mod\ 5).$$

b) $5 \cdot x \equiv 5 \ (mod\ 10)$

$$x \equiv 1 \ (mod\ 10) \text{ or } x \equiv 3 \ (mod\ 10) \text{ or } x \equiv 5 \ (mod\ 10) \text{ or}$$

$$x \equiv 7 \ (mod\ 10) \text{ or } x \equiv 9 \ (mod\ 10)$$

$$x \equiv 1 \ (mod\ 2).$$

c) $18 \cdot x \equiv 10 \ (mod\ 14)$

$$x \equiv 6 \ (mod\ 7)$$

Non-linear congruences

$x^2 + 3 \cdot x + 7 \equiv 0\ (mod\ 5)$ - solve this by brute force. There are only 5 cases to check.

Hint: write it as $x^2 + 3 \cdot x \equiv -7\ (mod\ 5)$.

Non-linear congruences

$x^2 + 3 \cdot x + 7 \equiv 0 \ (mod \ 5)$ - solve this by brute force. There are only 5 cases to check.

Hint: write it as $x^2 + 3 \cdot x \equiv -7 \ (mod \ 5)$.

x	x^2	$3x$	$x^2 + 3x$
0			
1			
2			
3			
4			

Non-linear congruences

$x^2 + 3 \cdot x + 7 \equiv 0 \ (mod \ 5)$ - solve this by brute force. There are only 5 cases to check.

Hint: write it as $x^2 + 3 \cdot x \equiv -7 \ (mod \ 5)$.

x	x^2	$3x$	$x^2 + 3x$
0	0		
1	1		
2	4		
3	4		
4	1		

Non-linear congruences

$x^2 + 3 \cdot x + 7 \equiv 0 \ (mod\ 5)$ - solve this by brute force. There are only 5 cases to check.

Hint: write it as $x^2 + 3 \cdot x \equiv -7 \ (mod\ 5)$.

x	x^2	$3x$	$x^2 + 3x$
0	0	0	
1	1	3	
2	4	1	
3	4	4	
4	1	2	

Non-linear congruences

$x^2 + 3 \cdot x + 7 \equiv 0 \ (mod\ 5)$ - solve this by brute force. There are only 5 cases to check.

Hint: write it as $x^2 + 3 \cdot x \equiv -7 \ (mod\ 5)$.

x	x^2	$3x$	$x^2 + 3x$
0	0	0	0
1	1	3	4
2	4	1	0
3	4	4	3
4	1	2	3

Non-linear congruences

$x^2 + 3 \cdot x + 7 \equiv 0 \ (mod \ 5)$ - solve this by brute force. There are only 5 cases to check.

Hint: write it as $x^2 + 3 \cdot x \equiv -7 \ (mod \ 5)$.

x	x^2	$3x$	$x^2 + 3x$
0	0	0	0
1	1	3	4
2	4	1	0
3	4	4	3
4	1	2	3