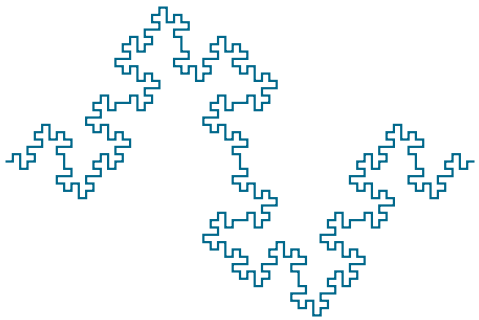
Cryptographic Mathematics I
Week 2

Dr. Eberhard Mayerhofer

University of Limerick



Semester I 2016/7

- A **prime** number p is an integer $p \geq 2$ whose only positive divisors are 1 and p.
- Positive integers greater than 2 which are not prime are called **composite**.
- Prime numbers less than 150 are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$$
$$53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$
$$101, 103, 107, 109, 113, 127, 131, 137, 139, 149$$

- All other positive integers less than 150 are composite. The following fact about prime numbers is very useful.

Euclid's Lemma

Theorem

Let p be a prime number which is a divisor of ab. Then either p is a divisor of a or p is a divisor of b or of both.

Proof:

- If p divides a we are done.
- If not, then $\gcd(p, a) = 1$. Thus by the result proved in the previous section there are integers r and s such that $ra + sp = 1$. Multiply through by b to get $rab + spb = b$. As p is a divisor of rab and of spb it is a divisor of $rab + spb = b$ as desired.

This property is not true of composite numbers e.g. 15 is a divisor of $33 \cdot 35$ but is neither a divisor of 33 nor of 35. Euclid's Lemma can be generalised as follows:

> *Let p be a prime number which is a divisor of the product $a_1 a_2 a_3 \cdots a_n$ of integers. Then p is a divisor of (at least) one of the factors $a_1, a_2, \ldots, a_n$.*

Theorem (Fundamental Theorem of Arithmetic)

Every integer $n \geq 2$ can be factored into a product of primes

$$n = p_1 p_2 \cdots p_m$$

in exactly one way. Different orders of the factors are not considered different.

Proof (Existence)

The proof is by induction on k.

- The case $k = 2$ is clearly true (why?)
- Inductive hypothesis: $P(k)$ every number up to k can be factored as a product of primes. Consider the number $k + 1$. If $k + 1$ is prime then we have a factorisation. If $k + 1$ is not prime then $k + 1 = n_1 n_2$ where $n_1, n_2 \leq k$. By the inductive hypothesis each of n_1 and n_2 can be written as a product of primes, say, $n_1 = p_1 p_2 \cdots p_r$ and $n_2 = q_1 q_2 \cdots q_s$. It follows that

$$k + 1 = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$$

is a factorisation into primes. Hence $P(k + 1)$ is true. Thus by induction $P(k)$ is true for all k.

Proof(Uniqueness)

Suppose that we have two different factorisations $n = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$. Consider p_1. The prime number p_1 divides n and so p_1 divides $q_1 q_2 \cdots q_s$. By Euclid's Lemma p_1 must divide q_k for some $1 \leq k \leq s$. But then $p_1 = q_k$. Renumber the factors in the second factorisation so that $p_1 = q_1$. Now cancel p_1 from each factorisation leaving $p_2 \cdots p_r = q_2 \cdots q_s$. Repeat the process starting with p_2. Eventually we will have all the ps paired off with one of the qs. When all the ps have gone all the qs must be gone otherwise $1 = q_m \cdots q_s$ which is impossible. Hence $r = s$. Thus the two factorisations are the same apart from the order of terms. This completes the proof.

Prime or Composite?

Natural questions:

- How can we determine if a number is prime or composite?
- If a number is composite how can we express it as a product of primes?

Some answers (upcoming)

- We will sometimes be able to show that a number is composite without necessarily finding a prime factor.
- We will also be able to find large prime numbers p and q such that given $n = pq$ it will be virtually impossible to find p and q.

Suppose one wants to find all prime numbers less than 200. Eratosthenes (276–194 BCE) devised a simple method to do this. Here is a brief description:

> *List the numbers from* 2 *to* 200. *For prime numbers* $p = 2, 3, 5, 11, 13$ *in turn delete all multiples of that prime except themselves. The integers that remain are all the primes less than* 200.

Why does this work? First note that any composite number that is not larger than a given number N must be divisible by a prime number $p \leq \sqrt{N}$, because the product of two or more primes greater than $\sqrt{N}$ is larger than N. Therefore, we only have to test the primes up to 13 when we want to find the primes up to 200.

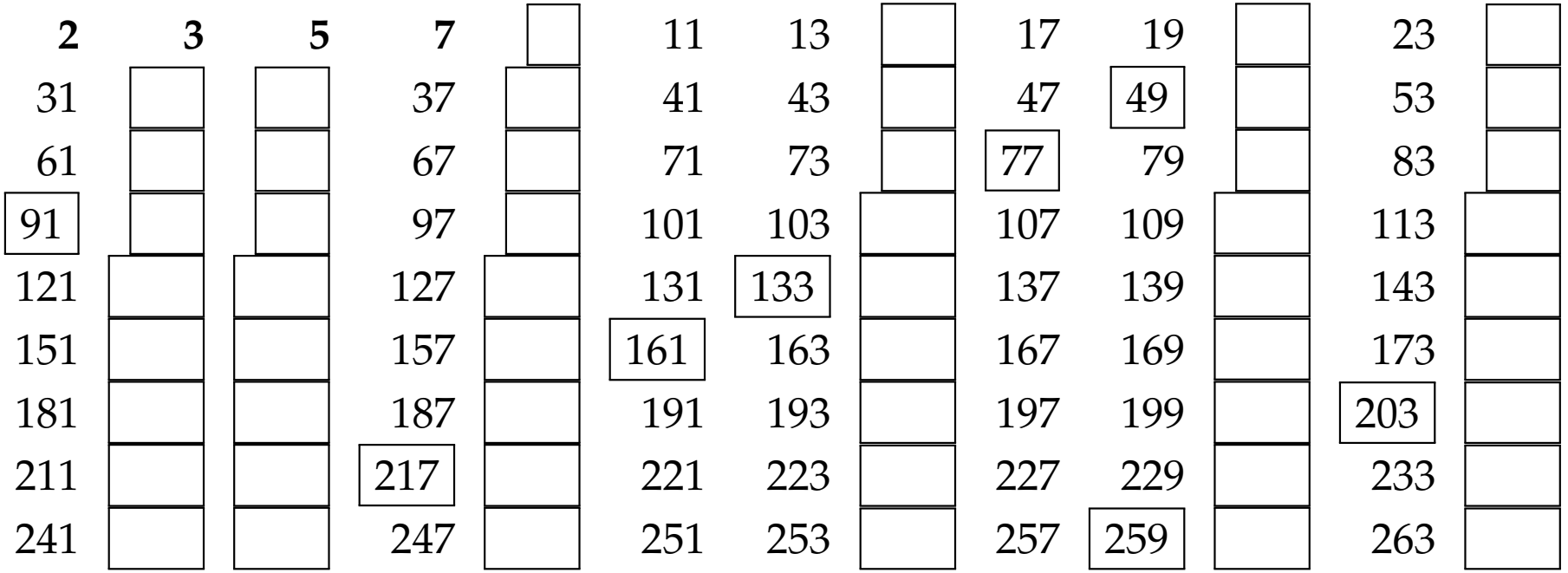
In practice, we first delete the multiples of 2, then those of 3 etc. simply by counting through the list in each case. In the example below, the result after eliminating all multiples of 2 is shown. The smallest remaining number is 3. This is a prime number. All multiples of 3 that are greater than 3 are marked with a box. They will fall through the sieve.

2	**3**	5	7	9	11	13	15	17	19	21	23	25	27	29
31	33	35	37	39	41	43	45	47	49	51	53	55	57	59
61	63	65	67	69	71	73	75	77	79	81	83	85	97	89
91	93	95	97	99	101	103	105	107	109	111	113	115	117	119
121	123	125	127	129	131	133	135	137	139	141	143	145	147	149
151	153	155	157	159	161	163	165	167	169	171	173	175	177	179
181	183	185	187	189	191	193	195	197	199	201	203	205	207	209
211	213	215	217	219	221	223	225	227	229	231	233	235	237	239
241	243	245	247	249	251	253	255	257	259	261	263	265	267	269

The next prime is 5 and now we mark the remaining multiples of 5 before they fall through the sieve.

2	**3**	**5**	7		11	13		17	19		23	25		29					
31		35	37		41	43		47	49		53	55		59					
61		65	67		71	73		77	79		83	85		89					
91		95	97		101	103		107	109		113	115		119					
121		125	127		131	133		137	139		143	145		149					
151		155	157		161	163		167	169		173	175		179					
181		185	187		191	193		197	199		203	205		209					
211		215	217		221	223		227	229		233	235		239					
241		245	247		251	253		257	259		263	265		269					

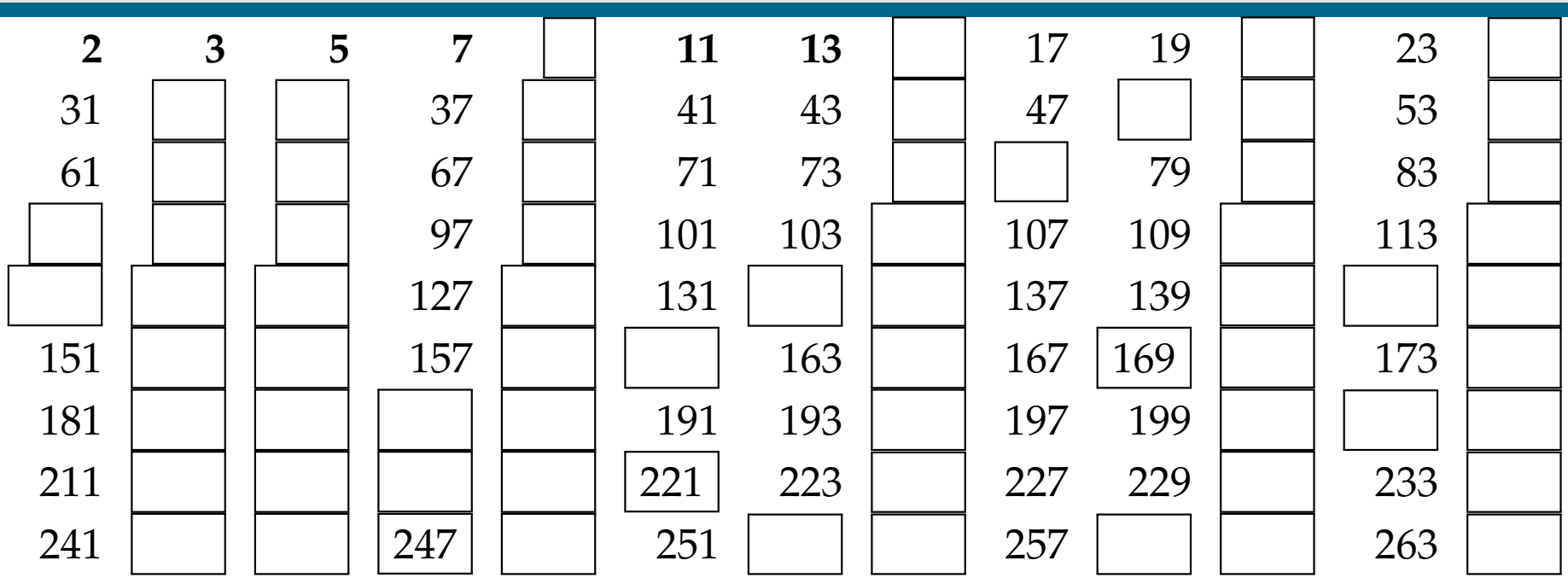
The next prime is 7 and now we mark multiples of 7 before they fall through the sieve.



The next prime is 11.

2	**3**	**5**	**7**		**11**	13		17	19		23	
31			37		41	43		47			53	
61			67		71	73			79		83	
			97		101	103		107	109		113	
121			127		131			137	139		143	
151			157			163		167	169		173	
181			187		191	193		197	199			
211					221	223		227	229		233	
241			247		251	253		257			263	

The next prime is 13 and the only new numbers that fall through the sieve are 169, 221 and 247.



Because $17^2 > 269$ all numbers in this table that didn't fall through the sieve so far must be prime numbers. With one more step we could have found all primes below $19^2 = 361$, but this would require that we included the numbers from 271 to 360 in all the steps we have carried out.

Recall: Properties

1. If $m \mid a$ and $m \mid b$ then $m \mid a+b$ and $m \mid a-b$.
2. If $m \mid a$ then $m \mid ka$ where k is an integer. Combining with 1) we have if $m \mid a$ and $m \mid b$ then $m \mid ka \pm lb$ for any integers k and l.
3. If $a \mid b$ and $b \mid c$ then $a \mid c$.
4. If $a \mid b$ and $c \mid d$ then $ac \mid bd$.
5. If $m \neq 0$ then $a \mid b \iff ma \mid mb$.
6. If $d \mid a$ and $a \neq 0$ then $|d| \leq |a|$.
7. $a \mid b$ and $b \mid a$ if and only if $a = \pm b$

Proof?

Divisibility is a key concept in number theory. We need a new notation to express divisibility concepts more easily.

Definition

We say that a **is congruent** to b **modulo** m if m divides $a - b$ and write this as

$$a \equiv b \mod m.$$

An expression involving $\equiv \mod m$ is called a **congruence**. For example

$$\begin{aligned} 21 &\equiv 9 \mod 12\,, \\ 2014 &\equiv 14 \mod 100\,, \\ 198 &\equiv 53 \mod 5\,, \\ -199 &\equiv 1 \mod 200\,. \end{aligned}$$

Given integers a and m, division with remainder gives us integers q, r such that $a = mq + r$ and $0 \leq r < m$. Then $a \equiv r \mod m$. Thus every integer is congruent modulo m to some number between 0 and $m - 1$.

Rules

We can handle congruences very much in the same way we handle equations. For example, if $a_1 \equiv b_1 \mod m$ and $a_2 \equiv b_2 \mod m$ then

$$\begin{aligned} a_1 + a_2 &\equiv b_1 + b_2 \mod m \\ a_1 - a_2 &\equiv b_1 - b_2 \mod m \\ a_1 a_2 &\equiv b_1 b_2 \mod m \\ a_1^n &\equiv b_1^n \mod m \quad \text{for all } n > 0. \end{aligned}$$

Division?

- $a \equiv b \mod m$, and $k \in \mathbb{Z}$ implies $ka \equiv kb \mod m$.
- We cannot, however, divide congruences in general:

$$20 \equiv 8 \mod 12 \qquad \text{but} \qquad 5 \not\equiv 2 \mod 12\,.$$

The following are, however, true.

- If $ak \equiv bk \mod m$ and $\gcd(k, m) = 1$ then $a \equiv b \mod m$. (Why?)
- If $ak \equiv bk \mod m$ and $k \mid m$ then $a \equiv b \mod \frac{m}{k}$. (Why?)

Solving congruence equations (Examples)

Cheap: One can use the exhaustive method i.e. to solve a congruence mod m one can try each value $0, 1, 2, \ldots, m-1$ in turn and determine those for which the congruence is true.

Example

To solve $x + 5 \equiv 2 \mod 12$, we may add 7 to both sides.

$$\begin{aligned} x + 5 + 7 &\equiv 2 + 7 \mod 12 \\ x + 12 &\equiv 9 \mod 12 \\ x &\equiv 9 \mod 12 \end{aligned}$$

This congruence has an infinite number of solution e.g. $x = 9, 21, 33, 45, \ldots$ and $x = -3, -15, -27, -39, \ldots$.

Example

To solve $3x + 4 \equiv 6 \mod 11$, we first subtract 4 from both sides, then multiply by 4 and finally use that $12 \equiv 1 \mod 11$.

$$\begin{aligned} 3x &\equiv 2 \mod 11 \\ 12x &\equiv 8 \mod 11 \\ x &\equiv 8 \mod 11 \end{aligned}$$

Note that here multiplication by 4 replaces division by 3 in the second step. How did we know that we have to multiply by 4? The key is $\gcd(11, 3) = 1$. The extended Euclidean algorithm gives

$$1 = 4 \cdot 3 - 11 \quad \text{i.e.} \quad 4 \cdot 3 \equiv 1 \mod 11 .$$

Example

To solve $x^2 + 3x + 5 \equiv 4 \mod 11$, we use the exhaustive method. Here we try $x = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ in turn and find the solutions

$$x \equiv 2 \mod 11 \quad \text{and} \quad x \equiv 6 \mod 11 .$$

Example

The congruence $x^2 \equiv 3 \mod 4$ does not have a solution. The reason is that for x even, we can write $x = 2k$, hence $x^2 = 4k^2 \equiv 0 \mod 4$ and for x odd, we can write $x = 2k + 1$, hence $x^2 = 4k^2 + 4k + 1 \equiv 1 \mod 4$. Squares can only have remainder 0 or 1 on division by 4, never 2 or 3.

Solving linear congruences

Consider the congruence

$$ax \equiv c \mod m$$

- This could have no solution e.g. take $a = 6, c = 9, m = 24$ (why?)
- Suppose our congruence has a solution x. Then $ax - c$ is a multiple of m and so $ax - c = my$ for some integer y. But then $ax - my = c$. We know that this has a solution if and only if $\gcd(a, m)$ divides c.

Let $d = \gcd(a, m)$ and suppose $au + mv = d$ then $a\frac{uc}{d} + m\frac{vc}{d} = c$. Because we assume that d divides c, the numbers $\frac{uc}{d}$ and $\frac{vc}{d}$ are integers. Hence

$$x_0 \equiv \frac{uc}{d} \mod m$$

is a solution to the congruence. Suppose x_1 is another solution. Then

$$ax_1 \equiv ax_0 \mod m\,.$$

Hence m divides $a(x_1 - x_0)$ and so $\frac{m}{d}$ divides $\frac{a(x_1-x_0)}{d}$. But $\gcd(\frac{m}{d}, \frac{a}{d}) = 1$. Thus $\frac{m}{d}$ divides $x_1 - x_0$. Hence

$$x_1 = x_0 + k\frac{m}{d}\,.$$

We can let k take the values $0, 1, 2, \ldots, d-1$ to obtain d different solutions.

Have just proved:

Theorem

Let a, c, m be integers with $m \geq 1$ and $d = \gcd(a, m)$.

1. *If d does not divide c then the congruence*

$$ax \equiv c \mod m$$

has no solutions.

2. *If $d \mid c$, then the congruence*

$$ax \equiv c \mod m$$

has exactly d incongruent solutions.

Recipe

To find the solutions, first use the extended Euclidean algorithm to find a solution (u_0, v_0) to the linear equation

$$au + mv = d.$$

Then $x_0 = \dfrac{cu_0}{d}$ is a solution of the congruence and a complete set of incongruent solutions is given by

$$x \equiv x_0 + k\frac{m}{d} \mod m \quad \text{for} \quad k = 0, 1, 2, \ldots, d-1.$$

Example

The congruence $10x \equiv 3 \mod 12$ has no solutions, because $\gcd(10, 12) = 2$ and $2 \nmid 3$.

Example

To solve $10x \equiv 6 \mod 12$, we observe that $\gcd(10, 12) = 2$ and $2|6$. Therefore we know that the congruence has two incongruent solutions. To find them, we first solve $10u + 12v = 2$. The solutions $u = -1, v = 1$ are easy to find. $u = 11, v = -9$ is also a solution. To find x_0 we need to multiply u by $6/2 = 3$:

$$x_0 = 3 \cdot 11 \equiv 33 \equiv 9 \mod 12\,.$$

The other solution is obtained by adding $12/2 = 6$, so we get

$$x_1 \equiv 9 + 6 \equiv 3 \mod 12$$

as the second solution. Thus the solutions to the congruence are

$$x \equiv 3 \mod 12 \quad \text{and} \quad x \equiv 9 \mod 12\,.$$

Example

Consider the congruence $126\,x \equiv 36 \mod 348$. Euclid's algorithm looks like this.

$$\begin{aligned} 348 &- 2 \cdot 126 &&= 96 \\ 126 &- 96 &&= 30 \\ 96 &- 3 \cdot 30 &&= 6 \\ 30 &- 5 \cdot 6 &&= 0 \end{aligned}$$

Therefore $\gcd(348, 126) = 6$. Because $6 \mid 36$ the given congruence has six solutions.

Whiteboard!