Section 4.3

Prime number

gcd: greatest ($\mathbb{Z}_+$) common devider

Sammen sat ↓ composite

Def 1: $a, b, c \in \mathbb{Z}$ $a \in \mathbb{Z}_+$. If $a = b \cdot c$ then a is composite

Ex: $18 = 3 \cdot 6$, so 18 is composite

$17 = ?.?$ No, 17 is prime

$b \geq 2, c \geq 2$

If a is not composite, then a is a prime number

$a \in \mathbb{Z}_+$ is prime iff the only divisor in $\mathbb{Z}$ are $a, -a, 1, -1$ and $a \neq 1$

1 is not a prime number because it has been decided.

Some primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, ...

Theorem 1: Every positive integer can be factorized into primes in a unique way

is prime? is prime?

$36 = 6 \cdot 6 = 3 \cdot 2 \cdot 3 \cdot 2$

$36 = 2 \cdot 18 = 2 \cdot 2 \cdot 9 = 2 \cdot 2 \cdot 3 \cdot 3$] the set of numbers here is unique to each integer

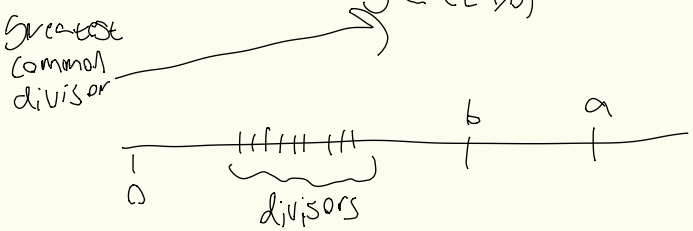
Theorem 2: If $n = \underbrace{p_1 \cdot p_2 \cdots p_k}_{\text{Primes } k \geq 2}$ then some $p_i \leq \sqrt{n}$

Def 2: $a, b, c \in \mathbb{Z}$, d is common divisor of a, b if $d|a$ and $d|b$

If $a > 0, b > 0$

d is then the greatest common divisor if d is greater than all the others

we write $d = gcd(a, b)$



Theorem 3: There are infinately many primes

Proof by contradiction: assume false

q_i: all primes All (primes): $p_1, p_2 \ldots p_n$

Consider: $p_1 \cdot p_2 \cdots p_n + 1 = q_1 \cdot q_2 \cdots q_k$

$q_i = p_i$ for some i

$1 = q_1 \cdots - p_1 p_2 \ldots p_i \ldots p_n$

$= p_i (\ldots - p_1 \cdot p_2 \ldots p_{i-1} \ldots p_n)$

some integer

1 can only be written as $-1 \cdot -1$ or $1 \cdot 1$

since primes are not negative and 1 is not prime we have a contradiction

Def: lcm = least common multiple

lcm(a,b) = The smallest number which is a multiple of a and b

---

Given a and b. Find gcd(a,b) and lcm(a,b)

Ex: if $a = 2 \cdot 3^2 \cdot 5 \cdot 11^2$ and $b = 2^2 \cdot 5 \cdot 7 \cdot 11$

The divisors of a and b are $2^{n_1}, 5^{n_2}, 11^{n_3}$

$gcd(a,b) = 2 \cdot 5 \cdot 11$ you only take of power 1 here because for its true value of one of them

$lcm(a,b) = 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11^2$

$\boxed{gcd(a,b) \cdot lcm(a,b) = a \cdot b}$

If you have 2 numbers a,b. Write them as primes

$a = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_n^{a_n}$

$b = p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_n^{b_n}$

you can have the same primes in a and b because it can just be in power 0, so it's 1 called the empty product $1 = p_1^0 \cdot p_2^0 \cdots p_n^0$

$gcd(a,b) = p_1^{\min(a_1,b_1)} \cdot p_2 \cdots p_n^{\min(a_n,b_n)}$

$lcm(a,b) = p_1 \cdot p_2 \cdots p_n^{\max(a_n,b_n)}$

This means $gcd(a,b) \cdot lcm(a,b) = p_1^{a_1+b_1} \cdot \ldots \cdot p_n^{a_n+b_n}$

Euclideans algorithm

Given $a,b \in \mathbb{Z}_+$ $a \geq b$ Find gcd(a,b)

Euclid: division algorithm

$a = b \cdot q_1 + r_2$ (focus on the remainders) $b > r_2 > r_3 > \ldots$

($a \to r_0$, $b \to r_1$)

replace r_0, r_1 with r_1, r_2

$b = r_2 \cdot q_2 + r_3$

$r_2 = r_3 \cdot q_3 + r_4$

$\vdots \quad \vdots \quad \vdots$ continue

$r_{n-1} = r_n \cdot q_n + 0$ you write 0 because the remainders become smaller, and we're dealing with positives integers.

$r_{n-3} = r_{n-2} \cdot q_{n-2} + r_{n-1}$

$r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n$ ← gcd(a,b)

Why is r_n the gcd?

Why is it r_n a common divisor?

Let us consider any divisor of a,b, say k

We will prove that $k | r_n$ and that $k | \text{all } r_i$

we know k is a divisor of a,b, then it also is of $a-b$, aka r_2. But we can then move b and r_2 over, so it also divides that and then also r_3. we can continue so it means it divides all r

Bezout's identity

$\alpha a + \beta b$ is a linear combination if $\alpha, \beta \in \mathbb{R}$
— " — an integer — " — $\alpha, \beta \in \mathbb{Z}$

says $d = r_n$ is an integer combination of a, b.
$d = \alpha a + \beta b$ where $\alpha, \beta \in \mathbb{Z}$ α, β are called Bezout coefficient

Looking at $r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n$, we know is an integer combination of r_{n-1}, r_{n-2}
and of r_{n-2}, r_{n-3}
and of r_{n-3}, r_{n-4}
⋮ ⋮
and of $r_1, r_0 = b, a$

Example

Find $\gcd(662, 414)$

$662 = 414 \cdot 1 + 248$
$414 = 248 \cdot 1 + 166$
$248 = 166 \cdot 1 + 82$
$166 = 82 \cdot 2 + 2$ ← gcd
$82 = 2 \cdot 41 + 0$

Now we'll work from the bottom and move

$2 = 166 - 82 \cdot 2 = 166 - (248 - 166) \cdot 2 = (-2)248 + 166 \cdot 3$
$= (-2)248 + (414 - 248) \cdot 3 =$
$= 414 \cdot 3 + 248(-5) = 414 \cdot 3 + (662 - 414)(-5)$
$= (-5)662 + 414 \cdot 8$

α ↑ ↑ β

you go 2 steps up and minus it

j	r_0	r_1	q_{j+1}	r_2	s_j	t_j
0	662	414	1	248	1	0
1	414	248	1	166	0	1
2	248	166	1	82	1	-1
3	166	82	2	2	-1	2
4	82	2	41	0	2	-3
					-5	10

↑ α ↑ β

Calculate the Bezout coefficient

$s_j = s_{j-2} - q_{j-1} \cdot s_{j-1}$

$t_j = t_{j-2} - q_{j-1} \cdot t_{j-1}$

Theorem

$a \mid b \cdot c \Rightarrow a \mid c$ it is true if $\gcd(a, b) = 1$

Everything is $\mathbb{Z}$

$b \cdot c = q \cdot a$

$\gcd(a, b) = 1$ means $1 = \alpha a + \beta \cdot b$ Multiply by c an integer. now c is a times something, so $a \mid c$

$c = \alpha ac + \beta bc = \alpha ac + \beta qa = a(\ldots)$ that is $a \mid c$ q.e.d.

Theorem

Suppose you have: $a \cdot b \equiv a \cdot c \pmod m \Rightarrow b \equiv c \pmod m$

True if $\gcd(a, m) = 1$

Proof

$m \mid ac - ab = a(c - b)$ (means) if $\gcd(a, m) = 1$, they are relatively prime. so one divides the other

so we know $m \mid c - b$ this means $c \equiv b \pmod m$

If m is prime and $a \neq 0$, then $\gcd(a, m) = 1$ is true

Opgaver

- **Section 4.3:** 3, 11, 15, 17, 31, 33, 41, 43, 49, 51, 55
- Prove that for any integer n > 1 and non-negative integer k, the integer n-1 divides n^k - 1.

11

$2^k = 3 \iff x \cdot \ln(2) = \ln(3) \iff x = \frac{\ln(2)}{\ln(3)}$

$\ln(2), \ln(3) \notin \mathbb{Z}$, så

17

a) yes. $\gcd(11,15)=1, \gcd(11,19)=1, \gcd(15,19)=1$

b) No. $\gcd(14,21)=7$

c) yes.

d) yes. $\gcd(8,9)=1$. Rest are coprime

31

Show that if a and $b \in \mathbb{Z}_+$, then $ab = \gcd(a,b) \cdot \mathrm{lcm}(a,b)$

$\gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdots p_n^{\min(\alpha_n,\beta_n)}$

$\mathrm{lcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdots p_n^{\max(\alpha_n,\beta_n)}$

$\mathrm{lcm}(a,b) \cdot \gcd(a,b) = p_n^{\min(\alpha_n,\beta_n)+\max(\alpha_n,\beta_n)} = p_n^{\alpha_n+\beta_n}$

33

Use the euclidean algorithm to find

a) $\gcd(12,18) = 6$

b) $\gcd(111,201) \iff 201 = 111 \cdot 1 + 90$
$111 = 90 \cdot 1 + 21$
$90 = 21 \cdot 4 + 6$
$21 = 6 \cdot 3 + 3 \leftarrow \gcd$
$6 = 3 \cdot 2 + 0$

c) $\gcd(1001,331) \iff 1331 = 1001 \cdot 1 + 330$
$1001 = 330 \cdot 3 + 11 \leftarrow \gcd$
$330 = 11 \cdot 30 + 0$

d) $\gcd(12345,54321) \iff 54321 = 12345 \cdot 4 + 4941$
$12345 = 4941 \cdot 2 + 2463$
$4941 = 2463 \cdot 2 + 15$
$2463 = 15 \cdot 164 + 3 \leftarrow \gcd$
$15 = 3 \cdot 5 + 0$

e) $\gcd(1000,5040) \iff 5040 = 1000 \cdot 5 + 40 \leftarrow \gcd$
$1000 = 40 \cdot 25 + 0$

f) $\gcd(9888,6060) \iff 9888 = 6060 \cdot 1 + 3828$
$6060 = 3828 \cdot 1 + 2232$
$3828 = 2232 \cdot 1 + 1596$
$2232 = 1596 \cdot 1 + 636$
$1596 = 636 \cdot 2 + 324$
$636 = 324 \cdot 1 + 312$
$324 = 312 \cdot 1 + 12 \leftarrow \gcd$
$312 = 12 \cdot 26 + 0$

43)

use the extended euclidean algoritamm to express gcd(144,89) as a linear comb. of 144 and 89

gcd(144,89) $\Leftrightarrow$ $144 = 89 \cdot 1 + 55$

$89 = 55 \cdot 1 + 34$

$55 = 34 \cdot 1 + 21$

$34 = 21 \cdot 1 + 13$

$21 = 13 \cdot 1 + 8$

$13 = 8 \cdot 1 + 5$

$8 = 5 \cdot 1 + 3$

$5 = 3 \cdot 1 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2 + 0$

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	144	89	1	55	1	0
1	89	55	1	34	0	1
2	55	34	1	21	1	-1
3	34	21	1	13	-1	2
4	21	13	1	8	2	-3
5	13	8	1	5	-3	5
6	8	5	1	3	5	-8
7	5	3	1	2	-8	13
8	3	2	1	1	13	-21
9	2	1	2	0	-21	34
10					34	-55

$-89 \cdot 144 + 144 \cdot 89$

$(34 \cdot 34 + (-55 \cdot 89)$

49

Prove that the product of any three consecutive integers is divisible by 6

$a, b, c \in \mathbb{Z}$

$a < b < c$

$abc \equiv 0 \pmod 6$

because every 2nd number is divisable by 2 and every 3rd is by 3, we can factorize

$a \cdot b \cdot c = 2 \cdot 3 \cdot (\dots) = 6 \cdot (\dots)$

↑ something

51) Prove or disprove that $n^2 - 79n + 1601$ is a prime whenever n is a positive integer

$1601^2 - 79 \cdot 1601 + 1601$ is not a prime

---

55)