math115A hw2

Jonas Chen

October 10, 1000

Problem 1

> Use the Euclidean algorithm to find the highest common factor of 18564 and 30030. Check your answer by writing each number as the product of prime powers. (proposition 1.5.5)

Solution

546, see handwritten notes

$30030 = 1 \times 18564 + 11466$
$18654 = 1 \times 11466 + 7098$
$11466 = 1 \times 7098 + 4368$
$7098 = 1 \times 4368 + 2730$
$4368 = 1 \times 2730 + 1638$
$2730 = 1 \times 1638 + 1092$
$1638 = 1 \times 1092 + 546$
$1092 = 2 \times 546 + 0$

Therefore the greatest common divisor (highest common factor) is 546.

Problem 2

> Granville, p. 36, Exercise 1.2.1.
> 1. Prove that if d divides both a and b, then d divides gcd(a, b)
> 2. Deduce that d divides both a and b if and only if d divides gcd(a, b)
> 3. Prove that 1 ≤ gcd(a, b) ≤ |a| and |b|
> 4. Prove that gcd(a, b) = |a| if and only if a divides b

Solution

a) We know that q_1, q_2 exist such that $a = q_1 d, b = q_2 d$.

From Granville theorem 1.1 we know that there exist u, v such that $\gcd(a, b) = au + bv$. Then

$$\gcd(a, b) = au + bv = (q_1 d)u + (q_2 d)v = d(q_1 u + q_2 v)$$

It follows that $d|d(q_1 u + q_2 v) \Rightarrow d| \gcd(a, b)$ since q_1, q_2, u, v must exist. $\square$

b) Want to show that $d|a \land d|b \Leftrightarrow d| \gcd(a, b)$

($\Rightarrow$) proven in part (a)
($\Leftarrow$) Suppose that $d| \gcd(a, b)$. Note that it must be true (since gcd is a divisor) that $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$. Then it follows that $d \mid a$ and $d \mid b$ (see the below note). $\square$

Note: if a divides b, and b divides c, then a divides c (excercise 1.1.1.e in Granville)

c) To show that $\gcd(a, b) \geq 1$, note that gcd is defined to be positive. Consider $a = q_1 \cdot \gcd(a, b), b = q_2 \cdot \gcd(a, b)$ then by lemma 1.1.1 (granville) the divisor $\gcd(a, b)$ must be greater than 1.

If $\gcd(a, b) = 0$ then $a = b = 0$ but $\gcd(0, 0)$ cannot be defined since there exists no largest integer n such that $0 \times n = 0$. Therefore $\gcd(a, b)$ cannot be 0.

If $\gcd(a, b) \leq 0$ we can simply use associativity to move the negative sign to the quotient, so that the gcd definition still holds.

To show that $\gcd(a, b) \leq |a|$ and $|b|$, first suppose on the contrary that $\gcd(a, b) > |a|$ or $\gcd(a, b) > |b|$.

Note that by lemma 1.1.1 there exists q_1, q_2 such that $a = q_1 \cdot \gcd(a, b)$ and $b = q_2 \cdot \gcd(a, b)$.

Consider the case then a is positive or negative. The assumption that $\gcd(a, b) > |a|$ guarantees that q_1 cannot exist. Similarly, q_2 cannot exist if b is positive or negative. This is a contradiction.

If $a = 0$ then $q_1 = 0$. We have $\gcd(0, b) = |b| \geq b$. However our assumption is that $\gcd(0, b) > b$, leading to a contradiction. (similar logic if we start with $b = 0$).

To conclude, we have $1 \leq \gcd(a, b) \leq |a|$ and $|b|$ $\square$

d) WTS: $\gcd(a, b) = |a| \Leftrightarrow a \mid b$

($\Rightarrow$) Suppose that $\gcd(a, b) = |a|$ then there exist q_1, q_2 such that $a = q_1\ |a|$ and $b = q_2\ |a|$. Clearly, $a \mid b$

($\Leftarrow$) Suppose that $a|b$. Note that $|a| \leq |b|$ by Exercise 1.1.1. (granville) Thus the greatest divisor that b shares with a is $|a|$. Additionally, the greatest divisor of a is $|a|$. Therefore $\gcd(a, b) = |a|$ $\square$

Note: `lemma` 1.1.1 is the division theorem.

Problem 3

> Granville, p. 36, Exercise 1.2.2.
> Suppose that a divides m, and b divides n
> 1. Deduce that gcd(a, b) divides gcd(m, n)
> 2. Deduce that if gcd(m, n) = 1, then gcd(a, b) = 1

Solution

Assumptions: $a \mid m$ and $b \mid n$

1.

Let $m = ak_1$ and $n = bk_2$ for some $k_1, k_2 \in \mathbb{Z}$. Also,let $a = \gcd(a, b) \cdot k_3$ and $b = \gcd(a, b) \cdot k_4$ for some $k_3, k_4 \in \mathbb{Z}$. Then

$$\gcd(m, n) = \gcd(ak_1, bk_2) = \gcd(\gcd(a, b) \cdot k_3 \cdot k_1, \gcd(a, b) \cdot k_4 \cdot k_2) = \gcd(a, b) \gcd(k_3 \cdot k_1, k_4 \cdot k_2)$$

and the claim follows. The last equality is due the fact that $\gcd(a, b) \geq 1$ by granville excercise 1.2.1(c) and is proven below and in granville Corollary 1.2.3 $\square$
2.

Follows from (1). Since the only integer factorization of 1 is 1×1 (and -1×-1) then it follows that $\gcd(a, b) = 1$, (also $\gcd(k_3 \cdot k_1, k_4 \cdot k_2) = 1$) $\square$

Another factorization of 1 is -1×-1 but gcd is defined to be positive so we cannot use this.

To follow up on part 1:
We would like to show the following property:
If m is a positive integer, then $\gcd(m \cdot a, m \cdot b) = m \cdot \gcd(a, b)$

consider $\gcd(m \cdot \gcd(a, b) \cdot k_1, m \cdot \gcd(a, b) \cdot k_2)$ where $a = \gcd(a, b) \cdot k_1, b = \gcd(a, b) \cdot k_2$. Then k_1, k_2 are coprime by the gcd definition, and we have $\gcd(m \cdot a, m \cdot b) = \gcd(m \cdot \gcd(a, b) \cdot k_1, m \cdot \gcd(a, b) \cdot k_2) = m \cdot \gcd(a, b)$

referencing the following: https://math.stackexchange.com/a/705888

Problem 4

> Which of the following Diophantine equations cannot be solved? (You should justify your answers.)
>
> a) $6x + 51y = 22$
> b) $33x + 14y = 115$
> c) $14x + 35y = 93$

Solution

a) cannot be solved, GCF is 3 but $3 \nmid 22$
b) can be solved, GCF is 1 and $1 \mid 115$
c) cannot be solved, GCF is 7 but $7 \nmid 93$

see handwritten notes

Problem 5

> Find a solution to the Diophantine equation $172x + 20y = 1000$

Solution

Using Euclidean algorithm we obtain
$x = 500, y = -4250$ is a solution

$172 = 8(20) + 12$
$20 = 1(12) + 8$
$12 = 1(8) + 4$
$8 = 2(4) + 0$

Then $\gcd(172, 20) = 4$ and $4 \mid 100 \Rightarrow$ can be solved.

Next we should solve $172x_i + 20y_i = 4$

First rearrange the equations from Euclidean algorithm:

$12 = 172 - 8(20)$
$8 = 20 - 1(12)$
$4 = 12 - 1(8)$
$0 = 8 - 2(4)$

Note thet

$$4 = 12 - 1(8) = 12(-20 - 12) = 2(12) - 20 = 2(172 - 8(20)) - 20 = 2(172) - 17(20)$$

Therefore $x_i = 2, y_i = -17$

The initial solution is $\left(x_i \cdot \frac{n}{d}, y_i \cdot \frac{n}{d}\right)$

Therefore a solution to this diophantine equation is $(2 \cdot 250, -17 \cdot 250) = (500, -4250)$

See the handwritten notes.

references:

https://math.libretexts.org/Courses/Mount_Royal_University/Higher_Arithmetic/5%3A_Diophantine_Equations/5.1%3A_Linear_Diophantine_Equations

https://brilliant.org/wiki/linear-diophantine-equations-one-equation/