

THE JOY OF NUMBERS

1. THE LAST WORD ON gcd

What we did today, was to go slowly over the proof of exercise 2(b) of the first test:

(1.1) **Exercise.** Let a, b , and c be three integers. If $gcd(a, b) = d$ and $gcd(b, c) = 1$, then $gcd(ab, c) = d$.

Proof. If we write all we know:

- (1) $gcd(a, c) = d$, implies that $a = dk_1$ and $b = dk_2$ with $gcd(k_1, k_2) = 1$;
- (2) $gcd(b, c) = 1$

we need to prove that $gcd(ab, c) = d$, with the substitutions in (1), what we need to prove is $gcd(dk_1b, dk_2) = d$. With some experiments, we decide that the following claim could be true, and very useful for our problem:

Claim 1: let m, p and l integers. $gcd(lm, lp) = lgcd(m, p)$.

If the claim holds true, what we need to prove is that $gcd(k_1b, k_2) = 1$. We decided to go by contradiction.

Assume that $gcd(k_1b, k_2) = r > 1$. Then

$$(1.1.1) \quad k_1b = rs_1$$

$$(1.1.2) \quad k_2 = rs_2,$$

for some integers s_1 and s_2 . Multiplying the equation 1.1.1 both side by s_2 and the equation 1.1.2 both side by s_1 , we obtain

$$s_2k_1b = rs_1s_2 = s_1k_2.$$

This says that $k_1|s_1k_2$. From the homework of two times ago, we have some information that help us, which we record as

Claim 2: if $gcd(m, n) = 1$ and $m|xn$ for some integer x then $m|n$.

Using this claim, we know that k_1 has to divide s_1 and in particular there exists an integer y such that $s_1 = yk_1$. if we substitute back in equation 1.1.1, we obtain:

$$k_1b = ryk_1,$$

so that $b = ry$. But r divides also k_2 since it is the $gcd(bk_1, k_2)$, in particular $k_2 = rt$, for some integer t . Since $c = dk_2$ we obtain that $c = drt$, and therefore r divides also c . So r divides c and b , but the $gcd(b, c) = 1$ and this implies that r has to be one, contradicting the assumption of $r > 1$. \square

This was an hard one. And we still haven't gone through. we need to prove the two claims:

Date: September 30, 2007.

Proof. Claim 1 Set $s = \gcd(m, p)$ and $t = \gcd(lm, lp)$. We need to prove that $ls = t$. We decide to go with an old trick: first prove that $ls \leq t$ and then $t \leq ls$. For the first one, since s divides both m and p , we have that ls divides both lm and lp . In particular ls is a common divisor between lm and lp . Since t is the greatest common divisor, we obtain $ls \leq t$.

For the other inequality, if $\gcd(m, p) = s$ then there are integers a and b such that $am + bp = s$, as the equation $mX + pY = s$ has solutions. Multiply both side by l , to obtain $lam + blp = ls$. In particular a and b are solutions also for the equation $lmX + lpY = ls$, and we know that this equation has solutions if and only if $\gcd(lm, lp)$ divides ls . This says that t divides ls and in particular $t \leq ls$. \square

Proof. Claim 2 Assume that $\gcd(b, c) = 1$ and c divides sb , then there exists an integer r such that $rc = sb$. by the assumption, the equation $bX + cY = 1$ has solutions, say h and k . In particular $bh + ck = 1$. Multiply both side by s to obtain $sbh + sck = s$. Substitute $sb = rc$ to obtain $rch + sck = s$ which reads $c(rh + sk) = s$, showing that c divides s . \square

Kelsey, showed us the proof of the following Theorem, which is a wonderful example of the power of a the proof by contradiction.

(1.2) **Theorem.** *There are infinitely many primes.*

Proof. Assume there are finitely many prime. we can list them all p_1, \dots, p_n . Consider the number $x = (p_1 p_2 \dots p_n) + 1$, in which we are adding one to the multiplication of all the primes (there are just finitely many of them). x is not a prime because is bigger then all the prime that exists: it is bigger then p_1, p_2 , up up to p_n . By the Theorem from last time we know that there exists a prime that divides x . This means that there exists an index i such that p_i divides x . So $p_i s = x$ and in particular

$$p_i s = p_1 \dots p_i \dots p_n + 1$$

But then $p_i(s - p_1 \dots p_{i-1} p_{i+1} \dots p_n) = 1$, implying that $p_i = 1$, which is a contradiction since p_i is prime and therefore strictly bigger then 1. \square

We decide that for a while there will be no more *gcd*.