A Basic Number Theoretic Result

Peter Borg

B.Sc. 2nd Year

Abstract: We are going to give a new proof that if the greatest common divisor of any two integers a and b is an integer t, then there must exist two integers x and y such that $t = xa + yb$.

First of all we are going to use the following symbols:

$\exists$	-	there exist/s
$\forall$	-	for all
gcd(a,b)	-	greatest common divisor of a and b
s.t.	-	such that
Z	-	set of integers
Z^+	-	set of positive integers

Putting the above statement in a more mathematical form we have:

If $\gcd(a,b) = t$, where $a, b, t \in Z$, then $\exists\ x, y \in Z$ s.t. $t = xa + yb$.

The following is the proof broken down into small parts:

- By definition $\gcd(a,b) = t$ means that there exist two integers λ and μ such that $\lambda t = a$ & $\mu t = b$.

  Now we claim - or rather we can show - that $\gcd(\lambda,\mu) = 1$.

  Suppose $\gcd(\lambda,\mu) = \alpha$ and $\alpha > 1$.

  $\therefore \exists\ \lambda 1, \mu 1 \in Z$ s.t. $\lambda 1 \alpha = \lambda$ and $\mu 1 \alpha = \mu$

  But $\lambda 1(\alpha t) = \lambda t = a$ and $\mu 1(\alpha t) = \mu t = b$

$\therefore$ gcd(a,b) = αt and $\alpha t > t$.

This is a contradiction because t is the greatest common divisor.

Hence, we have proved that gcd(λ,μ) = 1.

- We can reduce the problem to the following:

  To prove that $\exists$ x, y $\in$ Z s.t. $1 + y\mu = x\lambda$.

  This is because

  - if we are going to try to prove that $t = xa + yb$, we might as well divide throughout by t and try to prove that $\exists$ x, y $\in$ Z s.t. $x\lambda + y\mu = 1$, and
  - since y is any integer we can replace y by –y and get the modified
    statement.

- Suppose that $\forall$ x, y $\in$ Z $x\lambda + y\mu \neq 1$. This means that $1 + y\mu = x\lambda$ + r

  $\forall$ x, y $\in$ Z, where r $\in$ Z.

  Now, for any value of y we can find an x and an r such that $0 < r < \lambda$ (the basic division algorithm).

  This means that there are at most (λ - 1) different remainders.

- First, we should consider the special case $\lambda = 1$.

  In this case, put x = 1 and y = 0. Therefore r = 0. Hence, in this case, we have proved the original statement.

- Consider the following sequence of equations:

  $1 + 0\mu = 0\lambda + 1$

  $1 + 1\mu = x_1\lambda + r_1$

$1 + 2\mu = x_2\lambda + r_2$

...

$1 + n\mu = x_n\lambda + r_n$

...

We have solved the case for $\lambda = 1$. Now we should consider $\lambda \neq 1$.

Since there are at most $(\lambda - 1)$ different remainders:

$\exists\, i, j \in Z^+, j - i < \lambda$, s.t. $r_i = r_j$

$\therefore\ 1 + i\mu - x_i\lambda = 1 + j\mu - x_j\lambda$

$\therefore\ \mu(i - j) = \lambda(x_i - x_j)$

Since λ and μ have no common divisors (except 1) and $\lambda \neq 1$, the prime factorisation of λ should be contained in that of $(i - j)$. In other words, λ should divide $(j - i)$. But we know that $(j - i) < \lambda$. Hence λ does not divide $(j - i)$, and this gives a contradiction.

$\therefore$ there must exist a remainder which is equal to 0, i.e. $\exists\, r_k = 0$.

$\therefore\ \exists\, x_k, y_k \in Z$ s.t. $1 + y_k\mu = x_k\lambda$

$\therefore$ let $y = -y_k$ and $x = x_k$

$\therefore\ 1 = x\lambda + y\mu$

$\therefore$ multiplying throughout by t we get: $t = xa + yb$

$\therefore$ PROOF IS COMPLETE!

<u>Extension</u>: We can now go on to prove that if the greatest common divisor of two integers λ and μ is 1, then there exists an infinite number of pairs of integers x and y such that $x\lambda + y\mu = 1$.

Stated in mathematical terms, we have:

Suppose $\gcd(\lambda,\mu) = 1$, where $\lambda, \mu \in Z$, and that $(x,y) \in Z \times Z$ represents any pair of integers s.t. $x\lambda + y\mu = 1$. There exists an infinite number of pairs (x,y) s.t. $x\lambda + y\mu = 1$.

Note: The proof will consider only one infinite class of pairs:

- claim: $\gcd(x\lambda, y\mu) = 1$

  Suppose $\gcd(x\lambda, y\mu) = \alpha > 1$

  $\therefore \exists\ \alpha 1, \alpha 2 \in Z$ s.t. $\alpha 1\alpha = x\lambda$ and $\alpha 2\alpha = y\mu$

  $\therefore x\lambda + y\mu = \alpha 1\alpha + \alpha 2\alpha = \alpha(\alpha 1 + \alpha 2) = 1$

  $\therefore \alpha$ divides 1. This is a contradiction since $\alpha > 1$.

  $\therefore \gcd(x\lambda, y\mu) = 1$

- $\therefore \gcd(x^2\lambda, y^2\mu) = 1$

  $\therefore \exists\ p_1, q_1 \in Z$ s.t. $p_1(x^2\lambda) + q_1(y^2\mu) = 1$

  $\therefore$ Another pair is (p_1x^2, q_1y^2)

- $\therefore$ Similarly we can get other pairs

  $(p_nx^{n+1}, q_ny^{n+1}) \quad \forall n \in Z^+$