Greatest common divisor and the *Euclidean Algorithm*

Definition: Let $n \in \mathbf{N}$; then f is a *factor* of n if $f \in \mathbf{N}$ and $n = fF$ for some $F \in \mathbf{N}$.
Examples: 5 is a factor of 10, 12 is a factor of 12, 1 is a factor of 6, etc.

Definition: Let $a \in \mathbf{Z}$; then d is a *divisor* of a if $d \in \mathbf{Z}$, $d \neq 0$, and $a = dA$ for some $A \in \mathbf{Z}$.
Examples: 5 is a divisor of 10, -6 is a divisor of 12, 2 is a divisor of -6, etc.

Definition: If $a, b \in \mathbf{Z}$; then d is a *common divisor* of a and b if d is a divisor of both a and b.
Examples: 4 is a common divisor of 16 and 24, -2 is a common divisor of 16 and 24, 1 is a common divisor of 12 and 14, 10 is a common divisor of 10 and 20, etc.

Definition: If $a, b \in \mathbf{Z}$; then d is the *greatest common divisor* (usually abbreviated to gcd) of a and b if d is a common divisor of a and b, and $d' \leq d$ for *all* common divisors d' of a and b.
Examples: 8 is gcd of 16 and 24, 3 is the gcd of 15 and 24, 1 is the gcd of 12 and 17, 10 is the gcd of 10 and 20, etc.

Notation: If d is the greatest common divisor of a and b we write: $\gcd(a, b) = d$.

There is a *remarkable method* (and *no* faster method is known)–due to Euclid (known as the **Euclidean Algorithm**)–for finding the greatest common divisor of two integers. It is not just that this algorithm is fast from the point of view of actual numerical computation, but, much more importantly, it enables many fundamental results in Number Theory to be proved.

It is very striking that such a fundamentally important result is at the same time so simple. It all depends on the following elementary theorem:

Theorem 1: Let $a, b, q, r \in \mathbf{Z}$ with $a = bq + r$; then $\gcd(a, b) = \gcd(b, r)$.

I will give the proof in a moment, but first let me just comment on this Theorem1. You may think of it as saying this: 'if you divide an integer a by an integer b, getting quotient q and remainder r, then the greatest common divisor of the integers a and b is the same as the greatest common divisor of the integers b and r'.

You should appreciate the value of this observation. It means that the problem of finding the greatest common divisor of two integers a and b can be replaced by a simpler problem. How? Well, an example should make that immediately clear:

Example 1. Find $\gcd(987, 434)$.

Solution. Theorem 1 tells us that $\gcd(987, 434)$ equals $\gcd(434, r)$ where r is *any* integer such that $987\,(\text{namely } a) = 434\,(\text{namely } b) \times q + r$, with $q, r \in \mathbf{Z}$. There are several (infinitely many, actually) q's and r's for which the latter is true:

$$987 = 434.(-2) + 1855,$$
$$987 = 434.(-1) + 1421,$$
$$987 = 434.(0) + 987,$$
$$987 = 434.(1) + 553,$$
$$987 = 434.(2) + 119, \ \textit{etc.}$$

The *best* of these is $987 = 434.(2) + 119$, giving $\gcd(987, 434) = \gcd(434, 119)$. Then, *re-applying* Theorem1 $(434 = 119.3 + 77)$ gives: $\gcd(434, 119) = \gcd(119, 77)$. and a further use of Theorem 1 $(119 = 77.1 + 42)$ - we get that: $\gcd(119, 77) = \gcd(77, 42)$. Continuing in this manner we get:

$$\gcd(987, 434) = \gcd(434, 119) = \gcd(119, 77) = \gcd(77, 42) = \gcd(42, 35) = \gcd(35, 7) = 7.$$

It means that we have been able to calculate the greatest common divisor of two integers without having to find the actual divisors of either of them. The crucial thing is that at each stage the problem of finding the greatest common divisor of two integers was replaced by the *simpler* problem of finding the greatest common divisor of two *other* integers, the larger of which is the least of the previous two.

It is the application of Theorem1, and its *repeated* application, that constitutes what is called the ***Euclidean Algorithm***. We must first, however, prove that Theorem1. It is simple:

Proof of Theorem1. Let $\gcd(a, b) = d_1$ and $\gcd(b, r) = d_2$. (We want to prove that $d_1 = d_2$.)

Since d_1 is a common divisor of a and b then $a = d_1 A$ and $b = d_1 B$ for some $A, B \in \mathbf{Z}$, and so we have (from $a = bq + r$) that $d_1 A = (d_1 B)q + r$, and thus $r = d_1 A - (d_1 B)q = d_1(A - Bq)$. Thus d_1 is a divisor of r because $(A - Bq) \in \mathbf{Z}$, and, since d_1 is a divisor of b, it follows that d_1 is a common divisor of b and r. Therefore $d_1 \le d_2$. ... (*i*)

Also, d_2 is a common divisor of b and r, and so $b = d_2 B$ and $r = d_2 R$, for some $B, R \in \mathbf{Z}$, and so we have (from $a = bq + r$) that $a = (d_2 B)q + d_2 R$, and so $a = d_2(Bq + R)$. Thus d_2 is a divisor of a because $(Bq + R) \in \mathbf{Z}$, and, since d_2 is a divisor of b, it now follows that d_2 is a common divisor of a and b. Therefore $d_2 \le d_1$. ... (*ii*)

Between them, (i) and (ii) now give that $d_1 = d_2$, and so $\gcd(a, b) = \gcd(b, r)$. (**end of proof**.)

Easy? Yes, it is. Nothing could be simpler, and yet it very quickly leads to very important conclusions (I cannot think of anything that is so simple, but yet so important).

Note. In fact, *not only* is Theorem 1 true - namely that the greatest common divisor of a and b is equal to the greatest common divisor of b and r (given, of course, that $a = bq + r$) – *but* the

following is in fact true: *every* common divisor of *a* and *b* is a common divisor of *b* and *r*, and *vice versa*. That is:

Theorem 2: Let $a, b, q, r \in \mathbf{Z}$ with $a = bq + r,$ and let S_1 be the set of all common divisors of *a* and *b*, and S_2 be the set of all common divisors of *b* and *r*; then $S_1 = S_2$.

[I give a proof of this at the end of these notes; it is almost identical to the proof of Theorem 1.]

Now we are going to see how Theorem 1 leads to being able to find the greatest common divisor of any two integers. We will suppose from now on that $b > 0,$ and look first at the simplest case, namely the case where $b \mid a$. Here we immediately have that $\gcd(a, b) = b.$

Next we look at what happens when $b \nmid a$. Here we *choose* the remainder r_1 so that:

$$a = bq_1 + r_1, \text{and } 0 < r_1 \le (b-1), q_1 \in \mathbf{Z}.$$

Now we have that $\gcd(a, b) = \gcd(b, r_1),$ and now we do with *b* and r_1 what we just did with *a* and *b*, namely divide *b* by r_1. Why do we do this? Well, <u>if</u> $r_1 \mid b$ <u>then</u> $\gcd(b, r_1) = r_1,$ and so the value of $\gcd(a, b)$ would immediately be found from:

$$\gcd(a, b) = \gcd(b, r_1) = r_1.$$

But, if $r_1 \nmid b,$ and we *choose* the remainder r_2 so that:

$$b = r_1 q_2 + r_2, \text{ and } 0 < r_2 \le (r_1 - 1),\ q_2 \in \mathbf{Z},$$

we then have $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2).$

Then the problem is: what is the value of $\gcd(r_1, r_2)$? Again, if $r_2 \mid r_1$ then $\gcd(r_1, r_2) = r_2,$ and so the value of $\gcd(a, b)$ would immediately be found from:

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = r_2.$$

If, however, $r_2 \nmid r_1,$ then we continue as above, and perform yet another division:

$$r_1 = r_2 q_3 + r_3, \text{ and } 0 < r_3 \le (r_2 - 1),\ q_3 \in \mathbf{Z},$$

and - if necessary - perform several more similar divisions:

$$r_2 = r_3 q_4 + r_4, \text{ and } 0 < r_4 \le (r_3 - 1),\ q_4 \in \mathbf{Z},$$
$$r_3 = r_4 q_5 + r_5, \text{ and } 0 < r_5 \le (r_4 - 1),\ q_5 \in \mathbf{Z},$$
$$\cdots$$

with $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \gcd(r_3, r_4) = \gcd(r_4, r_5) = \ldots$

This sequence of equations *cannot* continue indefinitely. **Why?** Because '*a decreasing sequence of positive integers must have a least member*'. (This is sometimes referred to as the *Fundamental Property of the Natural Numbers*'). Here the decreasing sequence is $r_1, r_2, r_3, \ldots$.

Thus we must *eventually* arrive at *some* remainder r_n such that $r_n \mid r_{n-1}$, and so we end up with:

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, \text{ and } 0 < r_{n-1} \le (r_{n-2} - 1),\ q_{n-1} \in \mathbf{Z},$$
$$r_{n-2} = r_{n-1}q_n + r_n, \text{ and } 0 < r_n \le (r_{n-1} - 1),\ q_n \in \mathbf{Z},$$
$$r_{n-1} = r_n q_{n+1}, \text{ with } q_{n+1} \in \mathbf{Z}. \text{ (and thus } \gcd(r_{n-1}, r_n) = r_n.)$$

Finally we have: $\gcd(a, b) = \gcd(b, r_1) = \ldots = \gcd(r_{n-1}, r_n) = r_n$, and thus: $\underline{\underline{\gcd(a, b) = r_n}}$.

That last equation is of **fundamental importance** as it enables us to calculate - with incredible speed - the greatest common divisor of any two integers without having to calculate **any** common divisors at all!! It is a remarkable method due to Euclid (~ 300B.C.), and is rightly considered to be one of the very best *algorithms* (an *algorithm* - roughly speaking - is a set of instructions for carrying out a given calculation).

You should do - by hand - several worked examples of finding the greatest common divisor of two integers; examples like:

Find, using the *Euclidean Algorithm*, gcd(987, 345), gcd(12321, 337), gcd(97, 47), *etc*.

Note. **Maple** has an in-built command for calculating the gcd of any two integers; it is **igcd(a, b)**. This command (**igcd** for calculating the gcd of two ***i****ntegers*) happens to be one of a very small number whose **Maple** code cannot be accessed using the **interface(verboseproc=2)** (followed by **print(igcd)**) facility, but you will see in **Maple** lab classes a simple **Maple** procedure for calculating the gcd of any two integers.

Another very important related Maple command. There is a related command **igcdex**, which expresses the gcd of two integers as an '*integral linear combination*' of those integers. That is the subject of another set of notes.

Proof of Theorem 2. Let $f_1 \in S_1$ and $f_2 \in S_2$. (We will prove that $f_1 \in S_2$ and $f_2 \in S_1$, and so it will follow that $S_1 = S_2$.) Since $f_1 \in S_1$ then $a = f_1 A$ and $b = f_1 B$ for some $A, B \in \mathbf{Z}$, and so we have (from $a = bq + r$) that $f_1 A = (f_1 B)q + r$, and thus $r = f_1 A - (f_1 B)q = f_1(A - Bq)$. Thus f_1 is a divisor of r because $(A - Bq) \in \mathbf{Z}$, and, since f_1 is a divisor of b, it follows that f_1 is a common divisor of b and r. Thus every common divisor of a and b is also a common divisor of b and r,

$$i.e.\ f_1 \in S_2. \ \ldots (i)$$

Also, since $f_2 \in S_2$ then $b = f_2 B'$ and $r = f_2 R$, for some $B', R \in \mathbf{Z}$, and so we have (again from $a = bq + r$) that $a = (f_2 B')q + f_2 R$, and so $a = f_2(B'q + R)$. Thus f_2 is a divisor of a because $(B'q + R) \in \mathbf{Z}$, and, since f_2 is a divisor of b, it now follows that f_2 is a common divisor of a and b. Thus every common divisor of b and r is also a common divisor of a and b,

$$i.e.\ f_2 \in S_1.\ \ldots (ii)$$

Between them, (*i*) and (*ii*) now give that $S_1 = S_2$. (end of proof.)

The usual formal statement of the '*Euclidean Algorithm*' is this: Let $a, b \in \mathbf{Z}$ with $b > 0$. If $b \mid a$ then $\gcd(a, b) = d$; otherwise there are integers $q_1, r_1, q_2, r_2, \ldots, q_n, r_n, q_{n+1}$ such that:

$$\begin{aligned}
a &= bq_1 + r_1,\ 0 < r_1 \le (b-1),\\
b &= r_1 q_2 + r_2,\ 0 < r_2 \le (r_1 - 1),\\
r_1 &= r_2 q_3 + r_3,\ 0 < r_3 \le (r_2 - 1),\\
&\ \ \vdots\\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1},\ 0 < r_{n-1} \le (r_{n-2} - 1),\\
r_{n-2} &= r_{n-1} q_n + r_n,\ 0 < r_n \le (r_{n-1} - 1),\\
r_{n-1} &= r_n q_{n+1},
\end{aligned}$$

and $\gcd(a, b) = r_n$.
