Euclidean Algorithm

When we divide $b \mid a$ (q) remainder r this means $b(q) + r = a$ (by our method of checking division).

Because of this, if a number n is such that $n \mid a$ and $n \mid b$, then $n \mid r$.
[In words, if a number divides two numbers, it divides their remainder.]

See: $r = bq - a$.
$n \mid b$ implies $n \mid bq$ and $n \mid a$ implies $n \mid -a$
$n \mid bq$ and $n \mid -a$ implies that $n \mid bq + (-a)$ or $n \mid bq - a$, that is $n \mid r$.

We can use this fact to create a new way to find greatest common divisors. This method is called the Euclidean Algorithm. Given two numbers, for example 15 and 21. Let's find their greatest common divisor, call it $d = \gcd(15, 21)$.

If $d \mid 15$ and $d \mid 21$, then $d \mid r_1$ here $d \mid 6$.

If $d \mid 6$ and $d \mid 15$, then $d \mid r_2$ so $d \mid 3$.

If $d \mid 6$ and $d \mid 3$, then $d \mid r_3$ so $d \mid 0$, but this is obvious.

So, what the best thing we know is that $d \mid 3$. This means d is either 1 or 3. Nicely, all of these steps work backwards, because if a number divides the divisor and remainder of a division problem, then it divides the original number. Working backwards with 3 . .
$3 \mid 3$ and $3 \mid 0$, therefore $3 \mid 6$
$3 \mid 6$ and $3 \mid 3$, so $3 \mid 15$
$3 \mid 15$ and $3 \mid 6$, so $3 \mid 21$
Therefore $3 \mid 15$ and $3 \mid 21$. Since $3 \mid 15$ and $3 \mid 21$and $d \mid 3$, $d = 3$.

Notebook work: Use Euclidean Algorithm to find the greatest common divisor for each of these pairs. For each one, check the backwards proof as above.

(24, 42)
(210, 252)
(40, 72)
(22, 27)
(17, 51)

Sums of multiples

This work with the Euclidean Algorithm tells us a little more than just the greatest common divisor. For this reason, this is a particularly valuable method. Returning to our example of 15 and 21 . .

remember

$21 \div 15 = 1 \text{ r } 6$
$15 \div 6 = 2 \text{ r } 3$
$6 \div 3 = 2 \text{ r } 0$

Focus on the greatest common divisor, here 3. It first shows up as a remainder . . .

$2 (6) + 3 = 15$, that is $3 = 15 - 2 (6)$.

But, 6 also shows up as a remainder

$6 = 21 - 15$

So, $3 = 15 - 2(21 - 15) = 3(15) - 2(21) = 45 - 42 = 3$.

Ok, that's obvious, but there's something important here . .

$3 = 3 (15) - 2 (21)$, that is 3, the greatest common divisor, can be written as a sum of multiples of the two original numbers, 15 and 21.

By the same reasoning and computation, this is always true, that is the greatest common divisor can always be written as a sum of multiples of the two original numbers.

Notebook work: In each of the five examples used last time, write the greatest common divisor as the sum of multiples of the two original numbers.

Primes are Irreducible

Theorem: If p is a prime number, p | ab implies p | a or p | b.

Notebook work: This is not true if p is not prime. Create two counterexamples to this where p is not prime.

Proof of theorem: Assume p | ab.

We want to prove that either p | a or p | b. We'll start be assuming p † a, and prove p | b. If we can do this, we'll be done.

Notebook work: Explain briefly why this method of argument shows that if p | ab then p | a or p | b.

So assume p † a. Because p is prime, p has only 1 and p as factors. Therefore the greatest common divisor of p and a must be either 1 or p. But, here because p † a, the greatest common divisor of p and a must be 1 (otherwise it would be p and p would divide a).

By the previous page, we can thus write 1 as a sum of multiples of p and a:

$1 = sa + tp$

Multiply both sides by b:

$b = sab + tpb$

Now, we assumed p | ab, so it must be true that p | sab. Clearly p | tpb (this is clear, right?)

Notebook work: Why do we know if p | ab then p | sab?

So, p | sab and p | tpb, therefore p | sab + tpb = b, so p | b as desired.

Fundamental Theorem of Arithmetic: Prime factorization of natural numbers is unique up to order.

[This is the theorem that we use whenever we say "find *the* prime factorization of these numbers." Otherwise how do we know that there aren't seven different prime factorizations?]

Proof of FTA: Suppose that things labeled p_i are some prime numbers, and so are things labeled q_i.

Suppose that some number, $a \neq 1$, has two prime factorizations. Particularly suppose that $a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$. We want to show that the collection of primes in these lists is the same, maybe with a different order.

We see that $p_1 \mid a$. Therefore $p_1 \mid q_1 q_2 \cdots q_n$

By the theorem that says primes are irreducible, $p_1 \mid q_1$ or $p_1 \mid q_2 \cdots q_n$.

If $p_1 \mid q_1$, then $p_1 = q_1$.
If $p_1 \mid q_2 \cdots q_n$, then $p_1 \mid q_2$ or $p_1 \mid q_3 \cdots q_n$
and so on, eventually $p_1 \mid q_i$ for some i, and hence $p_1 = q_i$.

Divide both expressions for a by $p_1 = q_i$. Then repeat this procedure with p_2. This process matches prime factors on the left with prime factors on the right. Because it continues, it will match up all the prime factors until it is done. Then all the prime factors have been paired with each other, and it is shown that the two prime factorizations of a had the same prime factors.

This concludes the proof of the fundamental theorem of arithmetic.

Notebook work: Why did I assume $a \neq 1$? What about that case?