The Euclidean algorithm

Let $D(n)$ be the set of (positive) divisors of the natural number n, and let $CD(m,n)$ be the set of common divisors of m and n; that is, $CD(m,n) = D(m) \cap D(n)$. Then $\gcd(m,n)$ can be (and often is) defined as the maximum element of $CD(m,n)$. But it doesn't merely have the property that every element of $CD(m,n)$ is *less than or equal* to $\gcd(m,n)$; it has the stronger property that every element of $CD(m,n)$ is a *divisor* of $\gcd(m,n)$. So Doerr and Levasseur take the latter, stronger property to be the defining property of $\gcd(m,n)$. (It's obvious ahead of time that the finite set $CD(m,n)$ has a greatest element, but it's not so obvious that $CD(m,n)$ has an element that's a multiple of all the other elements! If you think it's "intuitively obvious" that $D(m) \cap D(n)$ must contain an element that's a multiple of other elements, explain why $D(m) \cap D(n)$ has this property while $D(m) \cup D(n)$ doesn't.)

Example: $D(12) = \{1,2,3,4,6,12\}$ and $D(20) = \{1,2,4,5,10,20\}$, so $CD(12,20) = D(12) \cap D(20) = \{1,2,4\}$ and $\gcd(12,20) = 4$.

One way to compute $\gcd(m,n)$ is to use the factorizations of m and n into primes: If $m = 2^{e_1}3^{e_2}5^{e_3}\cdots$ and $n = 2^{f_1}3^{f_2}5^{f_3}\cdots$ (where most of the exponents are zeroes!), then $\gcd(m,n) = 2^{g_1}3^{g_2}5^{g_3}\cdots$ where $g_i = \min(e_i, f_i)$ = whichever of e_i, f_i is smaller. For instance, $12 = 2^2 3^1 5^0 7^0 \cdots$ and $20 = 2^2 3^0 5^1 7^0 \cdots$ so $\gcd(12,20) = 2^{\min(2,2)} 3^{\min(1,0)} 5^{\min(0,1)} 7^{\min(0,0)} \cdots = 2^2 3^0 5^0 7^0 \cdots = 4$.

But when m and n are really large and hard to factor, a better way is the Euclidean algorithm. It is based on the following fact:

Claim: If $a = bq + r$, then $CD(a,b) = CD(b,r)$.

Application: $CD(20,12) = CD(12,8) = CD(8,4) = CD(4,0)$ (by repeated application of the Claim), and $CD(4,0) = D(4) = \{1,2,4\}$, so $\gcd(20,12) = 4$.

Proof of Claim:

(1) Suppose n is in $CD(a,b)$, so that $n|a$ and $n|b$. Since $a = bq + r$, $r = a - bq$ (that is, r can be expressed as a linear combination of a and b with integer coefficients). Since n divides a and n divides b, n divides both $(1)a$ and $(-q)b$ and therefore n divides their sum $(1)a + (-q)b$ which equals r. So $n|b$ and $n|r$. So n is in $CD(b,r)$. Hence $CD(a,b)$ is a subset of $CD(b,r)$.

(2) The proof that $CD(b,r)$ is a subset of $CD(a,b)$ is similar (and will be assigned for homework).

If we define $\gcd(a,b)$ as the largest element of $CD(a,b)$ (as I myself prefer to do), then we can show that for all positive integers c, if $c|a$ and $c|b$ then

$c|\gcd(a,b)$. That is, $(\forall c \in \mathbb{P})(c|a \ \wedge \ c|b \ \Rightarrow \ c|\gcd(a,b))$. We can also show that if k is any positive integer *other* than $\gcd(a,b)$, then it is *not* the case that $(\forall c \in \mathbb{P})(c|a \ \wedge \ c|b \ \Rightarrow \ c|k)$; that is, if $k \neq \gcd(a,b)$, then there exists an integer c that divides a and b but doesn't divide k. Putting it differently, $\gcd(a,b)$ is the *unique* integer k that satisfies $(\forall c \in \mathbb{P})(c|a \ \wedge \ c|b \ \Rightarrow \ c|k)$. That's why Doerr and Levasseur define gcd in this way. But note two defects of their definition: it's not obvious in advance that there are *any* such values of k, and it's not obvious in advance that there couldn't be *two or more* such values of k!

While we're talking about the gcd (greatest common divisor) we should also talk about the lcm (least common multiple). It's easiest to think about the relationship between the two in terms of prime factorizations: if $m = 2^{e_1}3^{e_2}5^{e_3}\cdots$ and $n = 2^{f_1}3^{f_2}5^{f_3}\cdots$, then, just as $\gcd(m,n) = 2^{g_1}3^{g_2}5^{g_3}\cdots$ where $g_i = \min(e_i, f_i) =$ whichever of e_i, f_i is smaller, we have $\operatorname{lcm}(m,n) = 2^{h_1}3^{h_2}5^{h_3}\cdots$ where $h_i = \max(e_i, f_i) =$ whichever of e_i, f_i is LARGER. As a consequence of the easily proved fact $\min(x,y) + \max(x,y) = x + y$, we have $\gcd(m,n)\operatorname{lcm}(m,n) = mn$. (Example: $\gcd(4,6) = 2$, $\operatorname{lcm}(4,6) = 12$, and $2 \times 12 = 4 \times 6$.) So, if you want to compute the least common multiple of two large numbers m and n, don't try to factor them into products of primes (which could be hard); instead, use the Euclidean algorithm to compute $\gcd(m,n)$, and then use the formula $\operatorname{lcm}(m,n) = mn/\gcd(m,n)$.

It's helpful to note that the Claim "If $a = bq + r$, then $CD(a,b) = CD(b,r)$" does not require that q be the quotient obtained when a is divided by b. In particular, setting $q = 1$ and $r = a - b$, we have the sometimes useful formula $CD(a,b) = CD(b, a - b)$.