If you happen to have the prime factorization of a and b in front of you, then it's very easy to write down $g.c.d.(a,b)$. Simply take all primes which occur in both factorizations raised to the minimum of the two exponents. For example, comparing the factorization $10780 = 2^2 \cdot 5 \cdot 7^2 \cdot 11$ with the above factorization of 4200, we see that $g.c.d.(4200, 10780) = 2^2 \cdot 5 \cdot 7 = 140$.

One also occasionally uses the *least common multiple* of a and b, denoted $l.c.m.(a,b)$. It is the smallest positive integer that both a and b divide. If you have the factorization of a and b, then you can get $l.c.m.(a,b)$ by taking all of the primes which occur in *either* factorization raised to the *maximum* of the exponents. It is easy to prove that $l.c.m.(a,b) = |ab|/g.c.d.(a,b)$.

The Euclidean algorithm. If you're working with very large numbers, it's likely that you won't know their prime factorizations. In fact, an important area of research in number theory is the search for quicker methods of factoring large integers. Fortunately, there's a relatively quick way to find $g.c.d.(a,b)$ even when you have no idea of the prime factors of a or b. It's called the *Euclidean algorithm.*

The Euclidean algorithm works as follows. To find $g.c.d.(a,b)$, where $a > b$, we first divide b into a and write down the quotient q_1 and the remainder r_1: $a = q_1 b + r_1$. Next, we perform a second division with b playing the role of a and r_1 playing the role of b: $b = q_2 r_1 + r_2$. Next, we divide r_2 into r_1: $r_1 = q_3 r_2 + r_3$. We continue in this way, each time dividing the last remainder into the second-to-last remainder, obtaining a new quotient and remainder. When we finally obtain a remainder that divides the previous remainder, we are done: that final nonzero remainder is the greatest common divisor of a and b.

Example 1. Find $g.c.d.(1547, 560)$.

Solution:

$$\begin{aligned} 1547 &= 2 \cdot 560 + 427 \\ 560 &= 1 \cdot 427 + 133 \\ 427 &= 3 \cdot 133 + 28 \\ 133 &= 4 \cdot 28 + 21 \\ 28 &= 1 \cdot 21 + 7. \end{aligned}$$

Since $7|21$, we are done: $g.c.d.(1547, 560) = 7$.

Proposition I.2.1. *The Euclidean algorithm always gives the greatest common divisor in a finite number of steps. In addition, for $a > b$*

$$\text{Time(finding } g.c.d.(a,b) \text{ by the Euclidean algorithm)} = O(log^3(a)).$$

Proof. The proof of the first assertion is given in detail in many elementary number theory textbooks, so we merely summarize the argument. First, it is easy to see that the remainders are strictly decreasing from one step to the next, and so must eventually reach zero. To see that the last remainder is the g.c.d., use the second definition of the g.c.d. That is, if any number divides both a and b, it must divide r_1, and then, since it divides