Solutions to In-Class Problems Week 8, Mon.

Problem 1.
A number is *perfect* if it is equal to the sum of its positive divisors, other than itself. For example, 6 is perfect, because $6 = 1 + 2 + 3$. Similarly, 28 is perfect, because $28 = 1 + 2 + 4 + 7 + 14$. Explain why $2^{k-1}(2^k - 1)$ is perfect when $2^k - 1$ is prime.[1]

Solution. If $2^k - 1$ is prime, then the only divisors of $2^{k-1}(2^k - 1)$ are:

$$1, \quad 2, \quad 4, \quad \ldots, \quad 2^{k-1}, \tag{1}$$

and

$$1 \cdot (2^k - 1), \quad 2 \cdot (2^k - 1), \quad 4 \cdot (2^k - 1), \quad \ldots, \quad 2^{k-2} \cdot (2^k - 1). \tag{2}$$

The sequence (1) sums to $2^k - 1$ (using the formula for a geometric series,[2] and likewise the sequence (2) sums to $(2^{k-1} - 1) \cdot (2^k - 1)$. Adding these two sums gives $2^{k-1}(2^k - 1)$, so the number is perfect. ■

Problem 2. (a) Use the Pulverizer to find integers x, y such that

$$x \cdot 50 + y \cdot 21 = \gcd(50, 21).$$

[1] Euclid proved this 2300 years ago. About 250 years ago, Euler proved the converse: *every* even perfect number is of this form (for a simple proof see http://primes.utm.edu/notes/proofs/EvenPerfect.html). As is typical in number theory, apparently simple results lie at the brink of the unknown. For example, it is not known if there are an infinite number of even perfect numbers or any odd perfect numbers at all.

[2] It's fun to notice the "Computer Science" proof that (1) sums to $2^k - 1$. The binary binary representation of 2^j is a 10^j, so the sum is represented by 1^k. This what you get by subtracting 1 from by 10^k which is the binary representation of 2^k.

Solution. Here is the table produced by the Pulverizer:

x	y	$\text{rem}(x,y)$	$=$	$x - q \cdot y$
50	21	8	$=$	$50 - 2 \cdot 21$
21	8	5	$=$	$21 - 2 \cdot 8$
			$=$	$21 - 2 \cdot (50 - 2 \cdot 21)$
			$=$	$-2 \cdot 50 + 5 \cdot 21$
8	5	3	$=$	$8 - 1 \cdot 5$
			$=$	$(50 - 2 \cdot 21) - 1 \cdot (-2 \cdot 50 + 5 \cdot 21)$
			$=$	$3 \cdot 50 - 7 \cdot 21$
5	3	2	$=$	$5 - 1 \cdot 3$
			$=$	$(-2 \cdot 50 + 5 \cdot 21) - 1 \cdot (3 \cdot 50 - 7 \cdot 21)$
			$=$	$-5 \cdot 50 + 12 \cdot 21$
3	2	1	$=$	$3 - 1 \cdot 2$
			$=$	$(3 \cdot 50 - 7 \cdot 21) - 1 \cdot (-5 \cdot 50 + 12 \cdot 21)$
			$=$	$\boxed{8 \cdot 50 - 19 \cdot 21}$
2	1	0		

■

(b) Now find integers x', y' with $y' > 0$ such that

$$x' \cdot 50 + y' \cdot 21 = \gcd(50, 21)$$

Solution. since $(x, y) = (8, -19)$ works, so does $(8 - 21n, -19 + 50n)$ for any $n \in \mathbb{Z}$, so letting $n = 1$, we have

$$-13 \cdot 50 + 31 \cdot 21 = 1$$

■

Problem 3.
For nonzero integers, a, b, prove the following properties of divisibility and GCD'S. (You may use the fact that $\gcd(a, b)$ is an integer linear combination of a and b. You may not appeal to uniqueness of prime factorization because the properties below are needed to *prove* unique factorization.)

(a) Every common divisor of a and b divides $\gcd(a, b)$.

Solution. For some s and t, $\gcd(a, b) = sa + tb$. Let c be a common divisor of a and b. Since $c \mid a$ and $c \mid b$, we have $a = kc, b = k'c$ so

$$sa + tb = skc + tk'c = c(sk + tk')$$

so $c \mid sa + tb$. ■

(b) If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

Solution. Since $\gcd(a, b) = 1$, we have $sa + tb = 1$ for some s, t. Multiplying by c, we have

$$sac + tbc = c$$

but a divides the second term of the sum since $a \mid bc$, and it obviously divides the first term, and therefore it divides the sum, which equals c.

■

(c) If $p \mid ab$ for some prime, p, then $p \mid a$ or $p \mid b$.

Solution. If p does not divide a, then since p is prime, $\gcd(p, a) = 1$. By part (b), we conclude that $p \mid b$. ■

(d) Let m be the smallest integer linear combination of a and b that is positive. Show that $m = \gcd(a, b)$.

Solution. Since $\gcd(a, b)$ is positive and an integer linear common of a and b, we have

$$m \leq \gcd(a, b).$$

On the other hand, since m is a linear combination of a and b, every common factor of a and b divides m. So in particular, $\gcd(a, b) \mid m$, which implies

$$\gcd(a, b) \leq m.$$

■

Appendix: The Pulverizer

Euclid's algorithm for finding the GCD of two numbers relies on repeated application of the equation:

$$\gcd(a, b) = \gcd(b, \text{rem}(a, b))$$

For example, we can compute the GCD of 259 and 70 as follows:

$$\begin{aligned}
\gcd(259, 70) &= \gcd(70, 49) && \text{since } \text{rem}(259, 70) = 49 \\
&= \gcd(49, 21) && \text{since } \text{rem}(70, 49) = 21 \\
&= \gcd(21, 7) && \text{since } \text{rem}(49, 21) = 7 \\
&= \gcd(7, 0) && \text{since } \text{rem}(21, 7) = 0 \\
&= 7.
\end{aligned}$$

The Pulverizer goes through the same steps, but requires some extra bookkeeping along the way: as we compute $\gcd(a, b)$, we keep track of how to write each of the remainders (49, 21, and 7, in the example) as a linear combination of a and b (this is worthwhile, because our objective is to write

the last nonzero remainder, which is the GCD, as such a linear combination). For our example, here is this extra bookkeeping:

x	y	$\text{rem}(x, y)$	$=$	$x - q \cdot y$
259	70	49	$=$	$259 - 3 \cdot 70$
70	49	21	$=$	$70 - 1 \cdot 49$
			$=$	$70 - 1 \cdot (259 - 3 \cdot 70)$
			$=$	$-1 \cdot 259 + 4 \cdot 70$
49	21	7	$=$	$49 - 2 \cdot 21$
			$=$	$(259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$
			$=$	$\boxed{3 \cdot 259 - 11 \cdot 70}$
21	7	0		

We began by initializing two variables, $x = a$ and $y = b$. In the first two columns above, we carried out Euclid's algorithm. At each step, we computed $\text{rem}(x, y)$, which can be written in the form $x - q \cdot y$. (Remember that the Division Algorithm says $x = q \cdot y + r$, where r is the remainder. We get $r = x - q \cdot y$ by rearranging terms.) Then we replaced x and y in this equation with equivalent linear combinations of a and b, which we already had computed. After simplifying, we were left with a linear combination of a and b that was equal to the remainder as desired. The final solution is boxed.

6.042J / 18.062J Mathematics for Computer Science
Spring 2010