Problem Set 2
Solutions

Foundations of Number Theory

Math 435, Fall 2006

1. (10+10+10 pts.) We have $5 = 2 \cdot 14 + 7$, $14 = 2 \cdot 7$, so $\gcd(14, 35) = 7$, and $7 = 35 - 2 \cdot 14$. Furthermore,

$$\begin{aligned} 15 &= 1 \cdot 11 + 4 \\ 11 &= 2 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 1 \cdot 3 \end{aligned}$$

so $\gcd(15, 11) = 1$, and $1 = -4 \cdot 11 + 3 \cdot 15$. Also

$$\begin{aligned} 4081 &= 1 \cdot 2585 + 1496 \\ 2585 &= 1 \cdot 1496 + 1089 \\ 1496 &= 1 \cdot 1089 + 407 \\ 1089 &= 2 \cdot 407 + 275 \\ 407 &= 1 \cdot 275 + 132 \\ 275 &= 2 \cdot 132 + 11 \\ 132 &= 12 \cdot 11 \end{aligned}$$

hence $\gcd(4081, 2585) = 11$. Moreover

$$\begin{aligned} 11 &= 275 - 2 \cdot 132 \\ &= 275 - 2 \cdot (407 - 1 \cdot 275) = 3 \cdot 275 - 2 \cdot 407 \\ &= 3(1089 - 2 \cdot 407) - 2 \cdot 407 = 3 \cdot 1089 - 8 \cdot 407 \\ &= 3 \cdot 1089 - 8(1496 - 1 \cdot 1089) = 11 \cdot 1089 - 8 \cdot 1496 \\ &= 11(2585 - 1 \cdot 1496) - 8 \cdot 1496 = 11 \cdot 1585 - 19 \cdot 1496 \\ &= 11 \cdot 2585 - 19(4081 - 1 \cdot 2585) = 30 \cdot 2585 - 19 \cdot 4081. \end{aligned}$$

2. (10+5+5 pts.) Let $a, b, c \in \mathbb{Z}$.
   (a) Let $d = \gcd(a, b)$. So we can write $a = ed$, $b = fd$ for some $e, f \in \mathbb{Z}$. Thus
   $$1 = sa + tb = s \cdot ed + t \cdot fd = (se + tf) \cdot d,$$
   hence $d = 1$. So a and b are coprime.
   (b) Suppose $\gcd(a, c) = \gcd(b, c) = 1$. So we can write
   $$1 = sa + tc = s'b + t'c \qquad \text{for some } s, t, s', t' \in \mathbb{Z}.$$

Now we have

$$\begin{aligned} 1 &= (sa + tc)(s'b + t'c) \\ &= ss'ab + st'ac + s'tbc + tt'c^2 \\ &= (ss') \cdot ab + (st'a + s'tb + tt'c) \cdot c. \end{aligned}$$

So ab and c are coprime by part (a).

(c) We proceed by induction on n. For $n = 1$ we have $F_n = F_1 = 1$, $F_{n+1} = F_2 = 1$, hence F_n and F_{n+1} are clearly coprime. Suppose that we have already shown that F_n and F_{n+1} are coprime; we have to show that F_{n+1} and F_{n+2} are coprime. There exist $s, t \in \mathbb{Z}$ such that $1 = aF_n + bF_{n+1}$. Now $F_n = F_{n+2} - F_{n+1}$, hence

$$1 = aF_n + bF_{n+1} = a(F_{n+2} - F_{n+1}) + bF_{n+1} = aF_{n+2} + (b - a)F_{n+1}.$$

By part (a), F_{n+2} and F_{n+1} are coprime.

3. (10 pts.) If $a|b$, then $\gcd(b, a) = a$; if $\gcd(b, x) = a$ for some x, then $a|b$. This shows (a) $\iff$ (c). If $a|b$, then $\mathrm{lcm}(a, b) = b$; and if $\mathrm{lcm}(a, y) = b$ for some y, then $a|b$. This shows (b) $\iff$ (c).

4. (20 pts.) We compute:

$$\begin{aligned} (2n + 1)^2 + (2n^2 + 2n)^2 &= (2n + 1)^2 + 4n^4 + 8n^3 + 4n^2 \\ &= (2n^2)^2 + 2 \cdot 2n^2 \cdot (2n + 1) + (2n + 1)^2 \\ &= (2n^2 + 2n + 1)^2. \end{aligned}$$

However, not every Pythagorean triple is of the form $(2n+1, 2n^2+2n, 2n^2+2n+1)$, $n > 0$; for example, $(15, 8, 17)$ is Pythagorean, but not of this form.

5. (20 pts.) We compute:

$$x^2 + y^2 = 4s^2t^2 + (s^4 + t^4 - 2s^2t^2) = 2s^2t^2 + s^4 + t^4 = (s^2 + t^2)^2 = z^2.$$

Hence (x, y, z) is Pythagorean. Note that since s, t are of opposite parity, both y and z are odd. Hence if p is a prime number with $p|y$ and $p|z$, then $p \neq 2$, and $p|y + z$, $p|z - y$, so $p|2s^2$ and $p|2t^2$. By Euclid's Lemma this yields $p|s$ and $p|t$, contradicting $\gcd(s, t) = 1$. Thus (x, y, z) is primitive. Suppose now $u, v \in \mathbb{N}$ yield the same triple (x, y, z), that is, $x = 2uv$, $y = u^2 - v^2$, $z = u^2 + v^2$. Then $2s^2 = y + z = 2u^2$, hence $s = u$, and $2t^2 = z - y = 2v^2$, hence $t = v$.

6. (20 pts. extra credit) Let $p > 2$ be a prime number. Then $p = 4k + 1$ or $p = 4k - 1$ for some $k \in \mathbb{N}$. Now note that $p^3 - p = (p - 1)p(p + 1)$. Hence if p is of the form $p = 4k + 1$ then

$$p^3 - p = (4k)(4k + 1)(4k + 2) = 8k(8k^2 + 6k + 1),$$

and one checks easily that one of k, $8k^2 + 6k + 1$ is divisible by 3, so $24|p^3 - p$. The case $p = 4k - 1$ is treated in a similar way.

Total: 100 pts. + 20 pts. extra credit.