

Math 406 – Fall 2009 – Harry Tamvakis
PROBLEM SET 2 – Due September 17, 2009
Grader - Allen Gehret

Reading for this week: Sections 1 and 2.

Problems

S1.2) Calculate $(3141, 1592)$ and $(10001, 100083)$.

Proof. Using the Euclidean Algorithm we get that

$$\begin{aligned}3141 &= 1592 + 1549 \\1592 &= 1549 + 43 \\1549 &= 36 \cdot 43 + 1 \\43 &= 43 \cdot 1 + 0\end{aligned}$$

and so $(3141, 1592) = 1$.

$$\begin{aligned}100083 &= 10 \cdot 10001 + 73 \\10001 &= 137 \cdot 73 + 0\end{aligned}$$

and so $(10001, 100083) = 73$. □

S1.4) Find x and y such that $4144x + 7696y = 592$.

Proof. First we calculate $(4144, 7696)$ by the Euclidean Algorithm

$$\begin{aligned}7696 &= 4144 + 3552 \\4144 &= 3552 + 592 \\3552 &= 6 \cdot 592 + 0\end{aligned}$$

and so $(4144, 7696) = 592$. Working backwards we see that

$$\begin{aligned}4144 - 3552 &= 592 \\4144 - (7696 - 4144) &= 592 \\2 \cdot 4144 - 7696 &= 592\end{aligned}$$

and so $x = 2$ and $y = -1$. □

S1.6) Find two different solutions of $299x + 247y = 13$.

Proof. First we calculate $(299, 247)$ using the Euclidean Algorithm

$$\begin{aligned}299 &= 247 + 52 \\247 &= 4 \cdot 52 + 39 \\52 &= 39 + 13 \\39 &= 3 \cdot 13 + 0\end{aligned}$$

and so $(299, 247) = 13$. Working backwards we get that

$$\begin{aligned}52 - 39 &= 13 \\52 - (247 - 4 \cdot 52) &= 13 \\5 \cdot 52 - 247 &= 13 \\5 \cdot (299 - 247) - 247 &= 13 \\5 \cdot 299 - 6 \cdot 247 &= 13\end{aligned}$$

and so one solution is $x = 5$ and $y = -6$. Any other solution is of the form $x = 5 + 19t$ and $y = -6 - 23t$ where $t \in \mathbb{Z}$ (by Theorem 1 on pg. 25). □

S1.11) (a) Prove that $(k, n + k) = 1$ if and only if $(k, n) = 1$.

Proof. (\Rightarrow) There exists $x, y \in \mathbb{Z}$ such that $kx + (n + k)y = 1$. Note that $(x + y)k + yn = 1$. Since $(x + y), y \in \mathbb{Z}$ we conclude that $(k, n) = 1$.

(\Leftarrow) There exists $x, y \in \mathbb{Z}$ such that $kx + ny = 1$. Note that $kx + ny = k(x - y + y) + ny = k(x - y) + (n + k)y$. Since $(x - y), y \in \mathbb{Z}$ we conclude that $(k, n + k) = 1$. □

(b) Is it true that $(k, n + k) = d$ if and only if $(k, n) = d$?

Proof. Yes. Let $(k, n+k) = d_1$ and $(k, n) = d_2$. Since $d_1 \mid k$ and $d_1 \mid n+k$ then $d_1 \mid n+k-k = n$. Since d_1 is a common divisor of n and k , we have that $d_1 \leq d_2 = (k, n)$. Conversely, since $d_2 \mid k$ and $d_2 \mid n$, then $d_2 \mid n+k$ so d_2 is a common divisor of both k and $n+k$. Thus $d_2 \leq d_1$. We conclude that $d_1 = d_2$. □

S2.2) Find the prime-power decompositions of 2345, 45670, and 999999999999. (Note that $101 \mid 1000001$.)

Proof.

$$2345 = 5 \cdot 7 \cdot 67$$

$$45670 = 2 \cdot 5 \cdot 4567$$

$$999999999999 = 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot 101 \cdot 9901$$

□

S2.3) Tartaglia (1556) claimed that the sums

$$1 + 2 + 4, \quad 1 + 2 + 4 + 8, \quad 1 + 2 + 4 + 8 \cdots$$

are alternatively prime and composite. Show that he was wrong.

Proof. The seventh sum, $1 + 2 + \cdots + 256$ *should* be prime (according to Tartaglia) but $511 = 7 \cdot 73$. □

S2.5) Prove that if n is square, then each exponent in its prime-power decomposition is even.

Proof. Assume $n = k^2$ where $k = p_1^{k_1} \cdot p_r^{k_r}$. Note that

$$\begin{aligned} k^2 &= (p_1^{k_1} \cdots p_r^{k_r}) (p_1^{k_1} \cdots p_r^{k_r}) \\ &= p_1^{k_1+k_1} \cdots p_r^{k_r+k_r} \\ &= p_1^{2k_1} \cdots p_r^{2k_r} \end{aligned}$$

has exponents of the form $2k_i$ for $1 \leq i \leq r$. Thus each exponent in the prime-power decomposition of n is even. □

S2.10) Prove that $n(n+1)$ is never a square for $n > 0$.

Proof. Note that for $n > 0$, $n^2 < n(n+1) < (n+1)^2$ and that n^2 and $(n+1)^2$ are consecutive squares. Since $n \mapsto n^2$ is strictly increasing, if $k < n$ then $k^2 < n^2 \neq n(n+1)$ and if $k > n+1$ then $k^2 > (n+1)^2 \neq n(n+1)$. Thus for all $k > 0$, $k^2 \neq n(n+1)$. \square

A1) a) In 1511, Carolus Bouvellus claimed that for $n \geq 1$ one or both of $6n-1$ and $6n+1$ were prime. Show that this conjecture is false.

Proof. Let $n = 20$. Note that $6 \cdot 20 - 1 = 119 = 7 \cdot 17$ and that $6 \cdot 20 + 1 = 121 = 11^2$. \square

b) Bouvellus must have realized something was amiss because he soon revised his claim to read that every prime, except 2 and 3, can be expressed in the form $6n \pm 1$, for some natural number n . Show that this conjecture is true.

Proof. Suppose $k = 6n + 2 > 3$. Then $k = 2 \cdot (3n + 1)$ and so $2 \mid k$.

Suppose $k = 6n + 3 > 3$. Then $k = 3 \cdot (2n + 1)$ and so $3 \mid k$.

Suppose $k = 6n + 4 > 3$. Then $k = 2 \cdot (3n + 4)$ and so $2 \mid k$. \square

c) Prove that $\{3, 5, 7\}$ is the only set of three consecutive odd numbers that are all prime.

Proof. Note that every set of three consecutive odd numbers is of one of the forms

$$\{6k + 1, 6k + 3, 6k + 5\},$$

$$\{6k + 3, 6k + 5, 6(k + 1) + 1\},$$

$$\{6k + 5, 6(k + 1) + 1, 6(k + 1) + 3\}.$$

Each of these sets contains an element which is divisible by 3. The only way this could possibly be all primes is if the term which is divisible by 3 is actually 3. This leaves $\{-1, 1, 3\}$, $\{1, 3, 5\}$ and $\{3, 5, 7\}$ as our only candidates but ± 1 are not prime so $\{3, 5, 7\}$ is the only set of three consecutive odd numbers that are all prime. \square

A2) a) How many natural numbers less than or equal to 1000 are divisible by 3? By 5? By 7?

Proof. (Assuming that 1 is the first natural number) the first number divisible by 3 is $3 \cdot 1$ and the last number divisible by 3 is $999 = 3 \cdot 333$ so the total number of natural numbers divisible by 3 in this interval is $333 - 1 + 1 = 333$.

The first number divisible by 5 is $5 \cdot 1$ and the last number divisible by 5 is $1000 = 5 \cdot 200$ so the total number of natural numbers divisible by 5 in this interval is $200 - 1 + 1 = 200$.

The first number divisible by 7 is $7 \cdot 1$ and the last number divisible by 7 is $994 = 7 \cdot 142$ so the total number of natural numbers divisible by 7 in this interval is $142 - 1 + 1 = 142$. \square

b) How many natural numbers less than or equal to 1000 are divisible by 3 or by 5?

Proof. First we count the number of natural numbers in this interval divisible by $3 \cdot 5 = 15$. Note that $15 \cdot 1$ is the first and $990 = 15 \cdot 66$ is the last so there are $66 - 1 + 1 = 66$ total. The total number of natural numbers divisible by 3 or 5 is $333 + 200 - 66 = 467$. We subtracted 66 because they represent the natural numbers that are counted twice, once for 3 and once for 5. \square

c) How many natural numbers less than or equal to 1000 are divisible by 3, 5, or 7?

Proof. We first count the number of natural numbers in this interval divisible by 21, 35 and 105.

For 21, the first is $21 \cdot 1$ and the last is $987 = 21 \cdot 47$ and the total is $47 - 1 + 1 = 47$.

For 35, the first is $35 \cdot 1$ and the last is $980 = 35 \cdot 28$ and the total is $28 - 1 + 1 = 28$.

For 105, the first is $105 \cdot 1$ and the last is $945 = 105 \cdot 9$ and the total is $9 - 1 + 1 = 9$.

The total number of natural numbers in this interval divisible by 3, 5 or 7 is $333 + 200 + 142 - 66 - 47 - 28 + 9 = 543$. The 9 is added back on to counteract elements which are accounted for 3 times and then unaccounted for 3 times. \square

A3) Prove that if $n > 4$ is composite, then n divides $(n - 1)!$. Conversely, show that if n is prime, then n does *not* divide $(n - 1)!$.

Proof. (\Rightarrow) Case 1. $n = ab$ for $1 < a, b$ and $a \neq b \leq n - 1$. Without loss of generality, $a < b$. Then $(n - 1)! = 1 \cdot 2 \cdots a \cdots b \cdots (n - 1)$ which implies that $n = ab \mid (n - 1)!$.

Case 2. $n = p^2$ for $1 < p < n - 1$. What we want to show here is that $(n - 1)!$ has 2 factors of p . This is only possible if $2p < n = p^2$ or rather $2 < p$. Since we require $n > 4$, this is fine.

(\Leftarrow) Assume not. Then by Lemma 6 since n is prime and $n \mid 1 \cdot 2 \cdots (n - 1)$ then $n \mid k$ for $1 \leq k \leq n - 1$. This is a contradiction since $n > k$.

□

A4) Find all prime numbers p such that $17p + 1$ is a perfect square.

Proof. Suppose $17p + 1 = k^2$ is a perfect square. Then $17p = (k + 1)(k - 1)$. Since $k \pm 1$ is an integer and 17 and p are both primes, we require that 17 equal one of $k \pm 1$ and p equal the other. The only possibilities for this is if $p = 15$ or $p = 19$. 15 is not prime and so $p = 19$ is the only prime number such that $17p + 1$ is a perfect square. □

Extra Credit Problems.

EC1) Determine, with proof, all prime numbers p such that $p + 10$ and $p + 20$ are also prime.

Proof. It is not difficult to show that one of $p, p + 10, p + 20$ will be divisible by 3. This leaves us with 3 options.

Option 1. Let $p = 3$ and then $p + 10 = 13$ and $p + 20 = 23$. This option works.

Option 2. Let $p + 10 = 3$ and then $p = -7$ and $p + 20 = 13$. This option works.

Option 3. Let $p + 20 = 3$ and then $p + 10 = -7$ and $p = -17$. This option works.

Thus $p \in \{3, -7, -17\}$. □

EC2) Let m and n be positive integers and suppose that a is an integer greater than 1. Use the Euclidean algorithm to prove that

$$\gcd(a^m - 1, a^n - 1) = a^{\gcd(m, n)} - 1.$$

Proof. □