Geoffrey Thomas
18.781 Problem Set 1
Collaborators: Liz Denys

1.2 2

$$\begin{aligned}1819 \times 0 + 3587 \times 1 &= 3587\\ 1819 \times 1 + 3587 \times 0 &= 1819\\ 1819 \times -1 + 3587 \times 1 &= 1768\\ 1819 \times 2 + 3587 \times -1 &= 51\\ 1819 \times -69 + 3587 \times 35 &= 34\\ 1819 \times 71 + 3587 \times -36 &= 17\end{aligned}$$

Since $17 \mid 34$, $(1819, 3587) = 17$, and we have the x and y values we want.

1.2 3

$$\begin{aligned}43 \times 0 + 64 \times 1 &= 64\\ 43 \times 1 + 64 \times 0 &= 43\\ 43 \times -1 + 64 \times 1 &= 21\\ 43 \times 3 + 64 \times -2 &= 1\end{aligned}$$

$$\begin{aligned}93 \times 1 - 81 \times 0 &= 93\\ 93 \times 0 - 81 \times -1 &= 81\\ 93 \times 1 - 81 \times 1 &= 12\\ 93 \times -6 - 81 \times -7 &= 9\\ 93 \times 7 - 81 \times 8 &= 3\end{aligned}$$

1.2 7 6, 10, and 15

1.2 13 $n^2 - n = n(n-1)$. Either n is even or $n-1$ is, ergo the product is divisible by 2.

$n^3 - n = (n-1)n(n+1)$. By the above reasoning, at least one of these terms is a multiple of 2. Similarly, at least one is a multiple of 3. So the product must have 6 as a factor.

$n^5 - n = n(n^2-1)(n^2+1) = (n-1)n(n+1)(n^2+1)$. By the above, the left three terms have 6 as a factor. Then, let n take the form $5q+r$ (with $q, r \in \mathbb{Z}$) by the division theorem. If $r \in \{0, 1, 4, 5\}$, then $(n-1)$, n, or $(n+1)$ is divisible by 5. Otherwise, $n^2+1 = 25q + 10qr + r^2 + 1$ is either $25q + 10qr + 5$ or $25q + 10qr + 10$, both of which are divisible by 5. Therefore the entire original product is always divisible by 5 and also by 6, so it is divisible by 30.

1.2 15 Let $x = 2a+1$ and $y = 2b+1$. Then $x^2 + y^2 = 4a^2 + 4b^2 + 4a + 4b + 2 = 4(a^2 + b^2 + a + b) + 2$, which has 2 as a factor, so $2 \mid x^2 + y^2$. By the division theorem, $q = a^2 + b^2 + a + b$ and $r = 2$ is the unique quotient and remainder of $(x^2 + y^2)/2$, and $r \neq 0$ means $4 \nmid x^2 + y^2$.

1.2 36 Let $x = (a, b)$. By definition $x \mid a$ and $x \mid b$. $((a, b), c) = (x, c)$, so $((a, b), c) \mid x$ and $((a, b), c) \mid c$. By the transitivity of the divisor relation (theorem 1.1), $((a, b), c) \mid a$ and b and is therefore a common divisor of a, b, and c. So by theorem 1.4, $((a, b), c) \mid (a, b, c)$.

On the other hand, since (a, b, c) is a common divisor of a and b, it divides (a, b). It also divides c, so by theorem 1.4 again, $(a, b, c) \mid ((a, b), c)$. But this combined with the previous result implies $((a, b), c) = (a, b, c)$.

1.2 49

$$\begin{aligned} a^{2^m}-1 &= \left(a^{2^{m-1}}+1\right)\left(a^{2^{m-1}}-1\right) \\ &= \left(a^{2^{m-1}}+1\right)\left(a^{2^{m-2}}+1\right)\left(a^{2^{m-2}}-1\right) \\ &= \left(a^{2^{m-1}}+1\right)\left(a^{2^{m-2}}+1\right)\cdots\left(a^2+1\right)(a+1)(a-1) \end{aligned}$$

Since $1 \le n < m$, $\left(a^{2^n}+1\right)$ is somewhere in this factorization.

1.2 53

$$\begin{aligned} &((n+1)!+1, n!+1) \\ &= ((n+1)!+1-(n+1)(n!+1), n!+1) \\ &= ((n+1)!+1-(n+1)!-n-1, n!+1) \\ &= (n, n!+1) \\ &= (n, n!+1-n(n-1)!) \\ &= (n,1) = 1 \end{aligned}$$

1.3 10 If $3k+2$ is prime, we are done; otherwise, write it as $a \times b$ for $a = 3c+d$ and $b = 3e+f$ where $0 \le a, b < 3k+2$ and $d, f \in \{0,1,2\}$, which we can do by the division theorem. Then $3k+2 = 9ce+3cf+3de+df$. Suppose that neither d nor f were 2; then df is either 0 or 1, which contradicts this equality (for all variables integers). So at least one of $a = 3c+2$ or $b = 3e+2$ must hold. Then repeat this argument on a and b until we find a prime, which we must because every integer factors into primes.

Similarly, let $4k+3 = (4a+b)(4c+d) = 16ac+4ad+4bc+bd$. for $b, d \in \{0,1,2,3\}$. If neither are 3, then $bd \in 0,1,2,4$, which again yields the equality unsolvable, so one must be 3.

Similarly, let $6k+5 = (6a+b)(6c+d) = 36ac+6ad+6bc+bd$ for $b, d \in \{0,1,2,3,4,5\}$. If neither are 5, then $bd \in \{0,1,2,3,4,6,8,9,12,16\} = \{0,1,2,3,4,6+0,6+2,6+3,12+0,12+4\}$, none of which, again, allow the equality to be solved, so one of them must be 5.

1.3 19 Write $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$, and $ab = \prod_p p^{\gamma(p)}$. Since $(a,b) = 1$, then if $\alpha p > 0$ then $\beta p = 0$ and vice versa (otherwise p would be a common divisor greater than 1). So since $\gamma p = \alpha p + \beta p$, γp is either αp or βp. Both of those are always even, since a and b are perfect squares, so γp is always even and c is a perfect square.

The same argument applies in in the general case in that αp and βp are always multiples of k, so since γp is always either one of them, it also is always a multiple of k, and so c is a kth power.

1.3 22

1. False, let $a = b = 2$ and $c = 4$, so $(a,b) = (a,c) = 2$, and $[a,b] = 2$ but $[a,c] = 4$.
2. True. The prime factorization of $(a,b) = (a,c)$ is unique, so in the product form, $\min(\alpha(p), \beta(p)) = \min(\alpha(p), \gamma(p))$. Because $\min(2x, 2y) = 2\min(x,y)$, then this means $\min(2\alpha(p), 2\beta(p)) = \min(2\alpha(p), 2\gamma(p))$, so $\left(a^2, b^2\right) = \left(a^2, c^2\right)$.
4. This means $a = jp$ and $a^2 + b^2 = kp$ for some positive integers j, k. Thus $j^2p^2 + b^2 = kp$, or $b^2 = p\left(k - j^2p\right)$, so $p \mid b \times b$, so $p \mid b$.
5. If $p \mid a^7$ then $p \mid aaaaaaa$, so $p \mid a$.
8. False, $8^2 \mid 4^3$ but $8 \nmid 4$.
12. Let $a = cd$ and $b = de$ where $d = (a,b)$. Therefore c and e are coprime (if not their common factor could be multiplied with d to yield an even greater common divisor). $\left[a^2, b^2\right] = \left[c^2d^2, d^2e^2\right]$. The gcd of these two numbers is d^2, so the lcm is $c^2d^2e^2$. Now consider $\left[a^2, ab, b^2\right] = \left[c^2d^2, cd^2e, d^2e^2\right]$. Its lcm must be at least $c^2d^2e^2$. But $cd^2e \mid c^2d^2e^2$, so that is in fact the lcm. Therefore $\left[a^2, b^2\right] = \left[a^2, ab, b^2\right]$.

1.3 26 Suppose there are a finite number of primes of the form $4n+3$. Consider the product of all of these primes; express the result in the form $4m+r$ for $0 \leq r < 4$. Now r is either 1 or 3, because any terms involving a $4n$ will be a multiple of 4, so r is the remainder of a power of 3 divided by 4, which is either 3 or 1. If r is 3, add 4 to it; otherwise add 2. Consider the prime factorization of the resulting number. It cannot contain any primes of the form $4n+3$, since by its construction, its remainder when divided by 3 is either 2 or 1, and its remainder when divided by any other such prime is either 2 or 4. However, this number cannot solely consist of factors of the form $4n+1$, since any product of those numbers would have the remainder 1 when divided by 4. And every prime other than 2 takes one of those two forms, and this odd number clearly does not have 2 as a factor. Therefore we have a contradiction of our ability to prime-factorize this number, so there must be an infinite number of primes of the form $4n+3$.

The above reasoning works in the $6n+5$ case; any product of numbers of the form $6n+r$ for $r \in \{1,3\}$ must also have remainder 1 or 3, and the only prime not of the form $6n+r$ for $r \in \{1,3,5\}$ is 2. So if there were a finite number of primes of the form $6n+5$, then the product of those numbers, plus the least nonzero offset needed to make the result itself have the form $6n+5$, would lead us to a contradiction when attempting to find its prime factors.

1.3 32

$$\begin{aligned}(n+1)^4+4 &= n^4+4n^3+6n^2+4n+5 &(1)\\ &= \left(n^4+4n^3+5n^2\right)+\left(n^2+4n+5\right) &(2)\\ &= \left(n^2+1\right)\left(n^2+4n+5\right) &(3)\end{aligned}$$

the two right terms of which are integers greater than one for any $n>0$, and therefore $(n+1)^4+4$ is composite for all such n.

1.3 37 Suppose in a block of integers there were two integers a and b both divisible by 2^i and no higher power of two, and no integer in the block were divisible by 2^{i+1}. Then we can write $a = c2^i$ and $b = d2^i$, where c and d are odd. But $c+1 < d$ (because d is odd) and is even, so $(c+1)2^i$ is divisible by 2^{i+1}, a contradiction. So in any block of integers there can be at most one integer divisible by some power of two 2^i where no other integer in the block is divisible by 2^{i+1}. However, in any nonempty block of integers is at least one integer divisible by 2^0 at least, so there must exist such an i and 2^i and integer divisible by it.

Somewhere in those fractions is the unique denominator described by the above property that is divisible by 2^i, where 2^i divides no other denominator. The simplified sum of the other elements has a denominator no greater than their least common denominator; the unique prime factorization of the lcd therefore has its power of 2 no greater than $i-1$, since the power is the maximum power of 2 across all the denominator. Let that fraction be written in that form $n/(d2^{i-1})$, where d is odd. Then

$$\frac{n}{d2^{i-1}} \pm \frac{1}{2^i} = \frac{2n \pm d}{d2^i}$$

Since the numerator is odd and the denominator is even, the quotient cannot be an integer.

1.3 39 This can be written

$$\sum_{n=1}^{2000} \frac{1}{n} - 2\sum_{n=1}^{1000} \frac{1}{2n}$$

in other words, starting with all the terms positive, then subtracting the even terms to cancel them, and then subtracting them again. But this is equal to

$$\sum_{n=1}^{2000} \frac{1}{n} - \sum_{n=1}^{1000} \frac{1}{n}$$

which is just

$$\sum_{n=1001}^{2000} \frac{1}{n}$$

QED.

1.3 48 Consider any two numbers $x = 2^{2^m} + 1$ and $y = 2^{2^n} + 1$, $m > n \geq 1$. Problem 1.2 49 tells us that $x-2 = 2^{2^m} - 1$ has a divisor of $y = 2^{2^n} + 1$, so given that $y \geq 5$, our first two numbers are coprime. But this holds between any two numbers x, y of that form, so all such numbers are coprime. Now suppose there were a finite number of primes $p_1 \ldots p_n$. Because all numbers in our sequence are coprime, i.e., they share no prime factors, they must partition these primes, such that any primes with a nonzero power in one number has a zero power elsewhere. But since all numbers in our sequence are greater than 1 and our sequence is infinite, we are looking for infinite partitions of a finite set, a contradiction. The only way to resolve it is let $p_1 \ldots$ be infinite.

3 We demonstrate the second claim, for which the first is an easy corollary: $m \mid n$ implies $(m, n) = m$ implies $a^{(m,n)} - 1 = a^m - 1$ implies $(a^m - 1, a^n - 1) = a^m - 1$ implies $a^m - 1 \mid a^n - 1$.

We can approach this with a variant of Euclid's algorithm. Let $m_0 = m$ and $n_0 = n$. Start with the two terms $a^{m_0} - 1$ and $a^{n_0} - 1$. At each step, if $m_i > n_i$, then subtract $a^{m_i - n_i}\,(a_i^n - 1)$ from the left term, leaving $a^{m_i - n_i} - 1$ as the new left term; if $n_i > m_i$, do the reverse. Terminate when the two terms are equal; this is the gcd, for the same reason that Euclid's algorithm terminates at the gcd (that $(a, b) = (a, b - ka)$ and $(a, a) = a$). Note that the m_i and n_i values followed the same structure as Euclid's algorithm, too, and the terms remained of the form $a^{m_i} - 1$ and $a^{n_i} - 1$. This final exponent is therefore (m, n), since the gcd is unique. And because we know that Euclid's algorithm will terminate at (m, n), we know that our variant will terminate, too.

Note that if $m \mid n$, $(a^n - 1) \,/\, (a^m - 1) = a^{n-m} + a^{n-2m} + a^{n-3m} + \cdots + 1$.

4 The following GP code does the calculations we want:

```
\p 6
a = b = c = 0;
for(start=0, 9, forprime(i=10000*start, 10000*(start+1), a++;
 b += (i == Mod(1, 4)); c += (i == Mod(3, 4))); print(a " " b
 " " c " " (10000*(start+1)/log(10000*(start+1)))))
```

Here are the results:

```
? \r hw1-4
   realprecision = 9 significant digits (6 digits displayed)
1229 609 619 1085.74
2262 1125 1136 2019.49
3245 1611 1633 2910.09
4203 2085 2117 3774.78
5133 2549 2583 4621.17
6057 3018 3038 5453.50
6935 3449 3485 6274.51
7837 3903 3933 7086.05
8713 4348 4364 7889.50
9592 4783 4808 8685.89
```

The balance between primes congruent to 1 and congruent to 3 modulo 4 is fairly close, with a slight but probably immaterial bias for 3. Growth seems roughly linear so far; it's not clear that $x/\log x$ is a better estimate yet.