Challenges

Anzo Teh Zhao Yang

December 21, 2016

1 Extra practice 1.

1. Let $n = 3k$. If k is odd then $k = 2x + 1$ for some $x \in \mathbb{Z}$. Now $2|n = 3(2x + 1) = 6x + 3 = 2(3x + 1) + 1$, so $2|1$, contradiction. Hence k is even and write $k = 2y$. Now $n = 3k = 3(2y) = 6y = 6 \times y$ so $6|6y = n$.
2. $a^2+b^2+c^2-ab-bc-ca = \frac{1}{2}((a-b)^2+(b-c)^2+(c-a)^2) \geq 0$, so $ab+bc+ca \leq a^2+b^2+c^2 = 1$. On the other hand $0 \leq (a+b+c)^2 = a^2+b^2+c^2+2ab+2bc+2ca = 1+2ab+2bc+2ca$, so $2(ab+bc+ca) \geq -1$, or $ab+bc+ca \geq \frac{-1}{2}$.

2 Extra practice 2.

1. We show that $p = 3$. Indeed, if $3|p$ then we must have $p = 3$, and if $3 \nmid p$ we have $p \equiv \pm 1 \pmod 3$ so $p^2 + 2 \equiv (\pm 1)^2 + 2 = 1 + 2 = 3 \equiv 0 \pmod 3$. This means $3 = p^2 + 2$, or $p = \pm 1$, contradiction. Hence $p = 3$, and $p^3 + 2 = 3^3 + 2 = 29$ is a prime.
2. In first order number theory we could write $\exists L(\forall \epsilon[0 < \epsilon \to (\exists \delta[0 < \delta \wedge (\forall x[0 < x + \delta \wedge x < \delta \to 3x + \epsilon < L \wedge 3x < L + \epsilon])])])$. Notice that this is unnecessarily complicated and hardly readable but in first order number theory only constants, variables, parenthesis, $\exists, \forall, \wedge, \vee, <, =$ are allowed. We could have written as $\exists L(\forall \epsilon > 0(\exists \delta > 0(|x| < \delta \to |3x - L| < \epsilon)))$.

   We show that $L = 0$ works (in fact, $L = 0$ is the only number you should think of). For each ϵ, choose $\delta = \frac{\epsilon}{3}$. Then $|x| < \delta \to |x| < \frac{\epsilon}{3} \to 3|x| < \epsilon to|3x| < \epsilon$.

3 Extra practice 3.

1. Suppose such a, b exist. From $a, b > 0$ we have $a^4 = b^4 + b + 1 > b^4 + b > b^4$, so $a > b$, and since $a, b \in \mathbb{Z}$ we have $a \geq b + 1$ by the discreteness property of the integers. Now $b^4 + b + 1 = a^4 \geq (b+1)^4 = b^4 + 4b^3 + 6b^2 + 4b + 1$, or $4b^3 + 6b^2 + 3b \leq 0$, contradicting that $b \geq 1$.
2. Let a, b, c be the side lengths, with c being the length of the hypothenuse. Given that $a^2 + b^2 = c^2$, we need to prove that one of a, b, c is divisible by 3. Suppose not, that $3 \nmid a, b, c$.

Then $a \equiv \pm 1 \pmod 3$ and $a^2 \equiv 1 \pmod 3$. Similarly $b^2 \equiv c^2 \equiv 1 \pmod 3$. Now from $2 = 1 + 1 \equiv a^2 + b^2 = c^2 \equiv 1 \pmod 3$, contradiction.

4 Extra practice 4.

1. *Existence.* We go by strong induction on each positive integer n. For $n = 1, 2, 3, 4, 5$ we can write them as $1, 2, 3, 1 + 3, 5$, respectively.

   Now let this statement to be true for $1, 2, \cdots, k - 1$ for some $k \geq 6$. Since the Fibanacci sequence F_i is unbounded and increasing, we can choose positive integer p such that p is the biggest positive integer with $F_p \leq k$. If $F_p = k$ we are done. Otherwise we have $F_p < k < F_{p+1} = F_p + F_{p-1}$, or $0 < k - F_p < F_{p-1}$. Now by our induction hypothesis, $k - Fp$ can be written as sum of distinct nonconsecutive Fibonacci numbers, namely $F_{i_1} + F_{i_2} + \cdots F_{i_x}$ for some $x \geq 1$, $i_1 < i_2 < \cdots i_x$ and $i_{j+1} - i_j \geq 2, \forall j \in [1, x - 1]$. But from $k - F_p < F_{p-1}$ we have $i_x < p - 1$. Therefore $k = F_{i_1} + F_{i_2} + \cdots F_{i_x} + F_p$ with $p - i_x \geq 2$.

   Uniqueness. We start with this claim:
   Let $1 < i_1 < \cdots i_x$ be integers satisfying $i_{j+1} - i_j \geq 2$ for all $j \in [1, x - 1]$. Then $F_{i_1} + F_{i_2} + \cdots F_{i_x} < F_{i_x+1}$.
   Proof: we proceed by induction. If $x = 1$ then we obviously have $F_{i_1} < F_{i_1+1}$ as $i_1 \geq 2$ (recall that $F_1 = F_2 = 1$ and $F_0 = 0$). Let us suppose that $F_{i_1} + F_{i_2} + \cdots F_{i_{x-1}} < F_{i_{x-1}+1}$. Then $F_{i_1} + F_{i_2} + \cdots F_{i_x} < F_{i_{x-1}+1} + F_{i_x} \leq F_{i_x-1} + F_{i_x} = F_{i_x+1}$ since $i_{x-1} \leq i_x - 2$. This completes the induction proof.

   Now we proceed with our main problem. Again we induct on n. For $n = 1$ our only choice is $F_2 = 1$. Now let $1, 2, \cdots k - 1$ to be written uniquely as sum of distinct non-consecutive Fibonacci numbers for some $k \geq 2$. Let p be the greatest positive integer with $F_p \leq k$, so $F_p \leq k < F_{p+1}$. Now let $F_{i_1} + F_{i_2} + \cdots F_{i_x}$ for some $x \geq 1$ and F_{i_j} be distinct non-consecutive Fibonacci numbers, with $1 < i_1 < \cdots i_x$. If $i_x > p$ then $F_{i_x} \geq F_{p+1} > k$ which is impossible. If $i_x < p$ then from above $F_{i_1} + F_{i_2} + \cdots F_{i_x} < F_{i_x+1} \leq F_p \leq k$, again a contradition. Hence $p = i_x$ and $F_{i_1} + F_{i_2} + \cdots F_{i_{x-1}} = k - F_p$. If $k = F_p$ then we are done, since there is no way to write 0 as sum of positive integers. If $k > F_p$ then by induction hypothesis $k - F_p$ can be writen uniquely as sum of distinct non-consecutive Fibonacci numbers, so $F_{i_1}, F_{i_2}, \cdots F_{i_{x-1}}$ can be determined uniquely.

5 Extra practice 5.

1. Let x be any divisor of $a - 1$. We claim that $x | n \Leftrightarrow x | \frac{a^n - 1}{a - 1}$. Indeed, since $a \equiv 1 \pmod x$, we have $\frac{a^n-1}{a-1} = a^{n-1} + a^{n-2} + \cdots a + 1 \equiv 1 + 1 + \cdots 1 (n \text{ times}) = n \pmod x$. So $\frac{a^n-1}{a-1} \equiv 0$ iff $n \equiv 0$, in modulo x, justifying the claim.

   Now if $x = \gcd(n, a - 1)$ then $x | n, x | a - 1$ and by the claim above, $x | \frac{a^n-1}{a-1}$ so x is a commn divisor of $\frac{a^n-1}{a-1}$ and $a - 1$, so $\gcd(n, a - 1) \leq \gcd(\frac{a^n-1}{a-1}, a - 1)$. Similarly, if $x = \gcd(\frac{a^n-1}{a-1}, a - 1)$ then $x | \frac{a^n-1}{a-1}$ and $x | a - 1$, so by the claim above $x | n$. Therefore $x = \gcd(\frac{a^n-1}{a-1}, a - 1)$ is the common divisor of n and $a-1$, so $\gcd(\frac{a^n-1}{a-1}, a-1) \leq \gcd(a-1, n)$. Combining the inequalties above yield $\gcd(\frac{a^n-1}{a-1}, a-1) = \gcd(a-1, n)$.

2. We claim that $\gcd(n, n+k) = k, \forall k \in [1, 20]$ by inducting on k. Now $\gcd(n, n+k) = \gcd(n, (n+k)-n) = \gcd(n, k) \leq k$. Therefore for base case $k=1$ we have $\gcd(n, n+1) \leq 1$ and since 1 divides both $n+1$ and n we have $\gcd(n, n+1) = 1$. Now suppose that $\gcd(n, n+i) = i$ for some $1 \leq i \leq 19$. Then $\gcd(n, n+i+1) > gcd(n, n+i) = i$ so $\gcd(n, n+1+1) \geq i+1$. On the other hand we have justifies that $\gcd(n, n+i+1) \leq i+1$ as of above. Therefore $\gcd(n, n+i+1) = i+1$, completing the induction claim.

   Now for all integers k with $1 \leq k \leq 20$ we have $\gcd(n, n+k) = k$ so $k|n, k|n+k$. This means $3|n, 7|n$ and since $\gcd(3,7) = 1$, lcm(3,7)$=3 \times 7 = 21$ so $21|n$ and $\gcd(n, n+21) = 21 > 20 = \gcd(n, n+20)$. Notice that the problem is true if we replace 21 with any number that is not a prime power.

3. First, we show that $2^x - 1|2^{xy} - 1$, $\forall x, y \geq 0$. Indeed, $2^x \equiv 1 \pmod{2^x - 1}$ so $2^{xy} = (2^x)^y \equiv 1^y \equiv 1 \pmod{2^x - 1}$. Therefore, since $\gcd(a, b)$ divides both a and b, we have $2^{\gcd(a,b)} - 1$ divides both $2^a - 1$ and $2^b - 1$, and therefore $2^{\gcd(a,b)} - 1 \leq \gcd(2^a - 1, 2^b - 1)$.

   Now first suppose that $a, b > 0$. To prove the other direction we need a corollary: for all odd positive integers x, if $x|2^a - 1$ and $x|2^b - 1$ then $x|2^{\gcd(a,b)} - 1$. Let d be the minimum positive integer such that $x|2^d - 1$ (this d exists because $x|2^{\phi(x)} - 1$ by Euler-Fermat theorem). We show that for all k, $x|2^k - 1 \Leftrightarrow d|k$. By Euclidean's remainder theorem we can write $k = bd + r$ with $0 \leq r < d$. Therefore $2^k = 2^{bd+r} = 2^{bd} \cdot 2^r = (2^d)^b \cdot 2^r =\equiv 1^b \cdot 2^r = 2^r$
   $pmodx$. If $r > 0$, then by the minimality of d we have $2^r \not\equiv 1 \pmod{x}$ but if $r = 0$, $2^r = 1$. Thus $x|2^d - 1 \Leftrightarrow x|2^r - 1 \Leftrightarrow r = 0 \Leftrightarrow d|k$.

   Now let's proceed with our claim, and here we let $x = \gcd(2^a - 1, 2^b - 1)$ (since 2 does not divide either of $2^a - 1, 2^b - 1$ for $a, b > 0$, $\gcd(2^a - 1, 2^b - 1)$ is also odd, so the claim above applies to this x.) If we define d as of above, the smallest positive integer with $x|2^d - 1$, then from $x|2^a - 1$ $x|2^b - 1$ we have $d|a$ and $d|b$. This would imply $d|pa + qb$ for all $p, q \in \mathbb{Z}$, and since there exists such p and q with $pa + qb = \gcd(a, b)$ by Euclidean algorithm, $d| \gcd(a, b)$. But this implies $x = \gcd(2^a - 1, 2^b - 1)|2^{\gcd(a,b)} - 1$, so $\gcd(2^a - 1, 2^b - 1) \leq 2^{\gcd(a,b)} - 1$. Summing the two inequalities we have $2^{\gcd(a,b)} - 1 = \gcd(2^a - 1, 2^b - 1)$ for a, b positive.

   In the case $a = 0$ then $2^{\gcd(a,b)} - 1 = 2^{\gcd(0,b)} - 1 = 2^b - 1 = \gcd(0, 2^b - 1) = \gcd(2^0 - 1, 2^b - 1) = \gcd(2^a - 1, 2^b - 1)$. The case $b = 0$ is completely analogous.

6 Extra practice 6.

1. (a) Yes, since 1+2+3+6=12=2×6.
   (b) No, since 1+7=8$\neq$ 14.
   (c) Since $2^k - 1$ is prime, all divisors of $n = 2^{k-1}(2^k - 1)$ can be written in the form of ab with $a = 2^i$ for some i with $0 \leq i \leq k-1$ and $b \in \{1, 2^k - 1\}$, due to the theorem of prime factorization. Therefore, the sum of divisors is
   $1 + (2^k - 1) + 2 + 2(2^k - 1) + \cdots + 2^{k-1} + (2^{k-1})(2^k - 1)$
   $= (1 + 2^k - 1) + 2(1 + 2^k - 1) + \cdots 2^{k-1}(1 + 2^k - 1)$

$= (1 + 2 + \cdots 2^{k-1})(1 + 2^k - 1)$
$= (2^k - 1)(2^k)$
$= 2(2^{k-1})(2^k - 1).$

Hence this number is perfect.

2. We denote $p_1, p_2, \cdots p_k$ as all the primes dividing either a or b or both. By theorem of prime factorization, we can write $a = \prod_{i=1}^{k} p_i^{a_i}$ and $b = \prod_{i=1}^{k} p_i^{b_i}$. Therefore $\gcd(a^n, b^n) = \gcd((\prod_{i=1}^{k} p_i^{a_i})^n, (\prod_{i=1}^{k} p_i^{b_i})^n) = \gcd(\prod_{i=1}^{k} p_i^{na_i}, \prod_{i=1}^{k} p_i^{nb_i}) = \prod_{i=1}^{k} p_i^{\min(na_i, nb_i)} = \prod_{i=1}^{k} p_i^{n\min(a_i,b_i)} = (\prod_{i=1}^{k} p_i^{\min(a_i,b_i)})^n$ $= (\gcd(a, b))^n$. Notice that we used the fact that $\min(nx, ny) = n\min(x, y)$ for $n \geq 0$ since if $x \leq y$ then $nx = ny = n(x - y) \leq 0$ so $nx \leq ny$ and $\min(nx, ny) = nx = n\min(x, y)$. Similarly if $x \geq y$ then $\min(nx, ny) = ny = n\min(x, y)$.

7 Extra practice 7.

1. Fo clarity we denote b_i as the digit appended on the end of a_{i-1} to orm a_i. We split into several senarios:
Scenario 1. If $b_i \in \{0, 2, 4, 6, 8\}$ for infinitely many i, then a_i is even for such i, hence composite. If b_i is 0 or 5 for infinitely many i then for such i, $5|a_i$, hence composite.

   Scenario 2. Suppose that scenario 1 didn't happen. Then there exists an N such that for all $k \geq N$ we have $b_k \in \{1, 3, 7\}$. Now further assume that for this scenario, $b_i \in \{1, 7\}$ infinitely many times. Then there exists sequence $N \leq c_1 < c_2 < \cdots$ such that for all $i \in \mathbb{N}$, we have $b_{c_i} \in \{1, 7\}$, so $b_{c_i} \equiv 1 \pmod 3$. Now if $c_x < j < c_{x+1}$ for some j, $b_j = 3$ by our definition of this sequence. Also let $a_{c_1} \equiv g \pmod 3$ for some $g \in \{0, 1, 2\}$. Now $a_{c_2} \equiv a_{c_1} + b_{c_1+1} + b_{c_1+2} + \cdots + b_{c_2} \equiv a_{c_1} + 3 + 3 + \cdots + 3 + 1 \equiv a_{c_1} + 1$ (we used the fact that for every integer n, n is equal to its sum of digits in modulo 3). Inductively, $a_{c_{i+1}} \equiv a_{c_i} + 1 \pmod 3$ so $a_{c_{i+1}} \equiv a_{c_1} + i \equiv g + i \pmod 3$. Now for all $i = 3k - g$ for $g \geq 1$, a_{c_i} is divisible by 3, so is composite.

   Scenario 3. Suppose that both scenarios 1 and 2 didn't happen, then there exists N such that for all $k \geq N$, $b_k = 3$. Let $m = a_N$, which ends with digit 3. If $3|m$ then $3|a_k$ for all $k \geq N$, so let's assume $3 \nmid m$. We can see that $\gcd(10, m) = 1$ since m is divisible by neither 2 nor 5. Now, by Euler's theorem, for all positive integers j, $10^{j\phi(m)} = (10^{\phi(m)})^j \equiv 1^j \equiv 1 \pmod m$, and we know the number $\underbrace{33\cdots3}_{j\phi(m) \text{ times}} = 3(\frac{10^{j\phi(m)}-1}{9}) = \frac{10^{j\phi(m)}-1}{3}$. is divisible by m since $m|10^{j\phi(m)} - 1$ and $\gcd(m, 3) = 1$. Now for all j, $a_{N+j\phi(m)} = a_N(10^{j\phi(m)}) + \frac{10^{j\phi(m)}-1}{3} = m(10^{j\phi(m)}) + \frac{10^{j\phi(m)}-1}{3}$ is divisible by m, hence is composite. Q.E.D.

2. We need this identity: The highest power of 2 that divides $3^{2^k} - 1$ is $k + 2$ for $k \geq 1$. Let's proceed by induction. If $k = 1$ then $3^{2^1} - 1 = 8 = 2^3 = 2^{1+2}$. Now suppose that the highest power of 2 dividing $3^{2^p} - 1$ is $p + 2$ for some $p \geq 1$. Then by induction hypothesis $3^{2^p} - 1 = c \cdot 2^{p+2}$ for some odd positive integer c. Now $3^{2^{p+1}} - 1 = (3^{2^p} - 1)(3^{2^p} + 1) =$

$c \cdot 2^{p+2} \cdot (c \cdot 2^{p+2} + 2) = c^2 \cdot 2^{2p+4} + c \cdot 2^{p+3}$. Now $\frac{c^2 \cdot 2^{2p+4} + c \cdot 2^{p+3}}{2^{p+3}} = c^2 \cdot 2^{p+1} + c$. Since $p \geq 1$, $c^2 \cdot 2^{p+1}$ is even but c is odd, so $c^2 \cdot 2^{p+1} + c = \frac{c^2 \cdot 2^{2p+4} + c \cdot 2^{p+3}}{2^{p+3}}$ is an odd integer, and thus the highest power of 2 dividing $3^{2^{p+1}} - 1$, completing the claim.

Now for the main problem we proceed by inducting on k. For $k = 1, 2, 3$ we can choose $n = 1$, so that $3 + 5 = 8$ is divisible by 2,4, and 8. Now suppose that for some $k \geq 3$, we can find n_k such that $2^k | 3^{n_k} + 5$. We want to prove that we can find n_{k+1} such that $2^{k+1} | 3^{n_{k+1}} + 5$. If $2^{k+1} | 3^{n_k} + 5$ then we can choose $n_{k+1} = n_k$. Otherwise, we can write $3^{n_k} + 5 = c \cdot 2^k$ for some odd c. Now choose $n_{k+1} = n_k + 2^{k-2}$. Recall that by above the highest power of 2 dividing $3^{2^{k-2}} - 1$ is k, so we can write $3^{2^{k-2}} - 1$ as $d \cdot 2^k$ for some odd d. Therefore, $3^{n_{k+1}} + 5 = 3^{n_k + 2^{k-2}} + (3^{n_k})(3^{2^{k-2}}) + 5 = (c \cdot 2^k - 5)(d \cdot 2^k + 1) + 5 = cd \cdot 2^{2k} - 5d \cdot 2^k + c \cdot 2^k - 5 + 5 = cd \cdot 2^{2k} + (c - 5d) \cdot 2^k = (2^{k+1})(cd \cdot 2^{k-1} + \frac{c-5d}{2})$. Now since $k \geq 3$, 2^{k-1} is an integer and since c and $5d$ are both odd, $c - 5d$ is even and therefore $\frac{c-5d}{2}$ is an integer. Therefore $cd \cdot 2^{k-1} + \frac{c-5d}{2}$ is an integer and $2^{k+1} | 3^{n_{k+1}} + 5$, completing the induction proof.

8 Extra practice 9.

1. Write $z = a + bi$ and $w = c + di$ for a, b, c, d real. Then:

   (a) $|z + w| = |(a + c) + (b + d)i| = \sqrt{(a + c)^2 + (b + d)^2}$ while $|z| + |w| = \sqrt{a^2 + b^2} + \sqrt{c^2 + d^2}$. By Cauchy-Schrawz inequality we have $(a^2 + b^2)(c^2 + d^2) \geq (ac + bd)^2$. Therefore
   $(\sqrt{(a + c)^2 + (b + d)^2})^2$
   $= (a + c)^2 + (b + d)^2$
   $= a^2 + b^2 + c^2 + d^2 + 2ac + 2bd$
   $\leq a^2 + b^2 + c^2 + d^2 + 2|ac + bd|$
   $= a^2 + b^2 + c^2 + d^2 + 2\sqrt{(ac + bd)^2}$
   $\leq a^2 + b^2 + c^2 + d^2 + 2\sqrt{(a^2 + b^2)(c^2 + d^2)}$
   $= (\sqrt{a^2 + b^2} + \sqrt{c^2 + d^2})^2$,
   so $|z + w| = |(a + c) + (b + d)i| = \sqrt{(a + c)^2 + (b + d)^2} \leq \sqrt{a^2 + b^2} + \sqrt{c^2 + d^2} = |z| + |w|$.

   (b) The right inequality is almost similar as above. For the left inequality, by (a) we have $|z| = |w + (z - w)| \leq |w| + |z - w|$ so $|z| - |w| \leq |z - w|$. Also $|w| = |z + (w - z)| \leq |z| + |w - z| = |z| + |z - w|$ (as $|a| = |-a|$ for all $a \in \mathbb{C}$) so $|w| - |z| \leq |z - w|$. Summing up both inequalities yield $||z| - |w|| \leq |z - w|$.

2. On the Cartesian plane, denote A, B, C as the coordinate corresponding to a, b, c on complex plane. Then in vector form $b - a = \overrightarrow{AB}$, $a - c = \overrightarrow{CA}$ and $c - b = \overrightarrow{BC}$. It suffices to prove that A, B, C either all coincide or are the vertices of an equilateral triangle. Observe $a - c$ and $c - b$ cannot be zero (otherwise the quotient may not be defined) so $\frac{b-a}{c-b} = \frac{a-c}{c-b} \neq 0$, and $b - a$ cannot be zero too. Thus no two point coincide.

   Let's consider the case where A, B, C are not collinear. Now we show that $\angle BAC = \angle ACB$. In subsequent solution we will talk about arg of vector in modulo 2π. Now, $\arg(b-a) - \arg(a-c) = \arg(\frac{b-a}{a-c}) = \arg(\frac{a-c}{c-b}) = \arg(a - c) - \arg(c - b)$. Also notice that $\arg(b - a) - \arg(a - c)$ is the counterclockwise angle needed to make vector $\overrightarrow{CA}$ parallel to (and heading the same direction with) $\overrightarrow{AB}$. Now, if A, B, C are in counterclowkwise order then $\arg(b-a) - \arg(a-c) =$

$\pi - \angle BAC$ and $\arg(a-c) - \arg(c-b) = \pi - \angle ACB$. Therefore $\angle BAC = \angle ACB$. If A, B, C are in clockwise order then $\arg(b-a) - \arg(a-c) = \pi + \angle BAC$ and $\arg(a-c) - \arg(c-b) = \pi + \angle ACB$. Therefore $\angle BAC = \angle ACB$. Now we have $|BC| = |AB|$, and $\frac{|AB|}{|CA|} = \frac{|CA|}{|BC|}$, or $|CA|^2 = |AB| \cdot |BC| = |AB| \cdot |AB| = |AB|^2$, so $|CA| = |AB|$.

If A, B, C are collinear (which holds vacuously when any two of them coincide) then $\arg(b-a) - \arg(a-c)$ and $\arg(a-c) - \arg(c-b)$ are both 0 or π. If they are 0 then $\overrightarrow{AB}, \overrightarrow{CA}, \overrightarrow{BC}$ are all pointing to the same direction, which is impossible. If they are π, then $\overrightarrow{AB}$ and $\overrightarrow{BC}$ are pointing at the same direction while $\overrightarrow{CA}$ pointing to the opposite direction. This means B is in between A and C and we have $|CA| = |AB| + |BC|$. Now $1 > \frac{|AB|}{|AB+BC|} = \frac{|AB|}{|CA|} = \frac{|CA|}{|BC|} = \frac{|AB+BC|}{|CA|} > 1$ since we assumed that $|CA|, |AB|, |BC| > 0$, contradiction.