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 (don't worry if you haven't heard of it; it's in MATH 145 syllabus) 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, $+, \times, \neg, \exists, \forall, \wedge, \vee, \to, \leftrightarrow, <, =$ 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 $2 = 1 + 1 \equiv a^2 + b^2 = c^2 \equiv 1 \pmod 3$, contradiction.

4 Extra practice 4.

1. Let's rephrase our problem into this form: For each positive integer n there exists a unique set $\{i_1, i_2, \cdots i_x\}$ such that $2 \leq i_1 < i_2 < \cdots < i_x$, $i_{j+1} - i_j \geq 2$ for all $j \in [1, x-1]$, and $n = F_{i_1} + F_{i_2} + \cdots F_{i_x}$ (we note that $F_2 = 1$).

   Existence. We go by strong induction on each positive integer n. Base cases: $1 = F_2, 2 = F_3, 3 = F_4, 1 + 3 = F_2 + F_4, 5 = F_5$. 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 $F_p = k$, write $k = F_p$. 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, $k - F_p = F_{i_1} + F_{i_2} + \cdots F_{i_x}$ for some $x \geq 1$, $2 \leq i_1 < i_2 < \cdots < i_x$ 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 $2 \leq i_1 < \cdots < i_x$ 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 inducting on x. If $x = 1$ then we obviously have $F_{i_1} < F_{i_1} + F_{i_1-1} = F_{i_1+1}$ as $F_{i_1-1} \geq F_1 = 1$. 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 $k \geq 2$. Suppose that $k = F_{i_1} + F_{i_2} + \cdots + F_{i_x} = F_{j_1} + F_{j_2} + \cdots + F_{j_y}$, with $2 \leq i_1 < i_2 < \cdots < i_x$, $i_{j+1} - i_j \geq 2$ for all $j \in [1, x-1]$ and $2 \leq j_1 < j_2 < \cdots < j_x$, $j_{w+1} - j_w \geq 2$ for all $w \in [1, y-1]$. Let p be the greatest positive integer with $F_p \leq k$, so $F_p \leq k < F_{p+1}$. If $i_x > p$ then $k = F_{i_1} + F_{i_2} + \cdots + F_{i_x} \geq F_{i_x} \geq F_{p+1} > k$ which is impossible. If $i_x < p$ then from above $k = F_{i_1} + F_{i_2} + \cdots F_{i_x} < F_{i_x+1} \leq F_p \leq k$, again a contradition. Hence $i_x = p$, and similarly $j_y = p$. If $F_p = k$ then we have $x = y = 1$ and $i_x = j_y = p$, so it has a unique representation in this case. Otherwise, we have $k - F_p = F_{i_1} + F_{i_2} + \cdots F_{i_{x-1}} = F_{j_1} + F_{j_2} + \cdots + F_{j_{y-1}}$. By induction hypothesis, $\{i_1, i_2, \cdots i_{x-1}\} = \{j_1, j)2, \cdots j_{y-1}\}$ so $\{i_1, i_2, \cdots i_x\} = \{i_1, i_2, \cdots i_{x-1}\} \cup \{p\} = \{j_1, j)2, \cdots j_{y-1}\} \cup \{p\} = \{j_1, j)2, \cdots j_y\}$, establishing the uniqueness for k.

2. **Answer.** $2^n - 1$.
   Denote the pegs as P_1, P_2, P_3 and denote the rings as $r_1, r_2, \cdots r_n$ where for all i, j with $i < j$ we have diameter of r_i less than that of r_j (which means r_1 on the top while r_n at the bottom.) Call $E(i, j \to k)$ as operation of moving r_i from P_j to P_k. Call pair of congiguration (C, C') *associative* if:

• C and C' are legal, i.e. no bigger ring is above smaller ring.
• For some $k \geq 1$, C has k rings and C' has $k+1$ rings (So in each associative pair the left element has one fewer ring than right element).
• For each $i \in [1,k]$, the location of r_i (i.e. in P_1, P_2 or P_3) is the same in boh C and C' (both in peg 1, both in peg 2, or both in peg 3).
We claim that for each associative pair (C, C') (with C having k ring and C' having $k+1$ rings), and each x, y, z with $x \in [1,k]$ and $y, z \in [1,3]$, $E(x, y \to z)$ is a valid move in C iff this same move is valid in C'. Moreover, if $E(x, y \to z)$ is valid in either case, and if D, D' are obtained from performing $E(x, y \to z)$ on C, C', respectively, (D, D') is associative. (Meaning that operations on rings $r_1, r_2, \cdots, r_k$ preserve associativity.)

Proof: Let $E(x, y \to z)$ be a valid move in C. This means r_x is originally at P_y and is on the top of P_y, so no ring in P_y is smaller than r_x. Since the move to P_z is valid, no ring in P_z is smaller than r_x. Hence, each r_i with $i < x$ must be at a peg other than P_y and P_z. Now consider C', and by the definition of associativity with C we know that in C', r_x is originally at P_y and for all $i < x$, since $x \leq k$ we have $i < k$ so r_i is on a peg other than P_y and P_z. Consequently, P_y and P_z has all rings larger or equal to r_x, so it is legal to move r_x from P_y to P_z. Now the (D, D') is associative, since both configurations are legal, and all rings are still in the same position (as compared with C and C') except for r_x, which are both in P_z. The case where $E(x, y \to z)$ is completely analogous provided that $x \leq k$.$\Box$

We proceed to our main problem by inducting on n. For $n = 1$ it is straightforward to see that all we need to do is to move the only ring to one of the other pegs, hence one step needed (and we cannot do it in 0 step, so 1 step is minimum).

Now suppose that for some k, the minimal number of steps required is $2^k - 1$. W.L.O.G. let $r_1, r_2, \cdots, r_{k+1}$ be in P_1. Denote this configuration as C'. Throughout the solution we introduce C as the configuration such that (C, C') is associative. The associativity holds troughout our whole process as all operations preserve associativity (this is true even when r_{k+1} is moved in C' and nothing is done in C as we will see later). First we show that $2^{k+1} - 1$ steps is attainable. Now in C there exists operations $P(x_1, y_1 \to z_1)$, $P(x_2, y_2 \to z_2)$, $\cdots$, $P(x_{2^k-1}, y_{2^k-1} \to z_{2^k-1})$ that moves all $r_1, r_2, \cdots, r_k$ to peg 2. It follows that we can apply $E(x_1, y_1 \to z_1)$, $E(x_2, y_2 \to z_2)$, $\cdots$, $E(x_{2^k-1}, y_{2^k-1} \to z_{2^k-1})$ to C'. Moreover, all rings $r_1, r_2, \cdots, r_k$ in C' are now in P_2. Now we haven't touched r_{k+1} in C' yet, so we can place it at P_3, Since associativity is independent of the position of r_{k+1} in C', (C, C') is still associative ater this move (we do nothing on C for this round). By symmetry there exists a $2^k - 1$-step operation in C to move all rings from P_2 to P_3, so this is the same for C' as well.The total number of steps is therefore $(2^k - 1) + 1 + (2^k - 1) = 2(2^k) - 1 = 2^{k+1} - 1$.

Let's now show that $2^{k+1} - 1$ is the minimum. First, notice that our task requires us to move r_{k+1} from P_1 to other peg. Suppose that we move this ring at step $g + 1$. To do so, all $r_1, r_2, \cdots, r_k$ must have been moved to other pegs. Moreover, one of the pegs 2 or 3 must be empty, since the r_{k+1} has the largst radius and cannot be placed on the other rings. W.L.O.G. we assume that peg 3 is empty. This means there exist operations $P(x_1, y_1 \to z_1)$, $P(x_2, y_2 \to z_2)$, $\cdots$, $P(x_g, y_g \to z_g)$ involving $r_1, r_2, \cdots, r_k$ in C'. Now in C the exact sequence of operations $P(x_1, y_1 \to z_1)$, $P(x_2, y_2 \to z_2)$, $\cdots$, $P(x_g, y_g \to z_g)$ also move all first k rings to P_2 (as associativity is preserved at all times), and by inductive hypothesis this requires at least 2^k-1 steps. Thus $g \geq 2^k-1$. Now at step $g+1$ we move r_{k+1} to P_3. Let the additional number of steps needs as h and consider the sequence of the next h steps $P(x_{g+2}, y_{g+2} \to z_{g+2})$, $P(x_{g+3}, y_{g+3} \to z_{g+3})$, $\cdots$, $P(x_{g+h+1}, y_{g+h+1} \to z_{g+h+1})$. If the final position (after h steps) of the rings are at P_3 (for C') then during the h steps we have already moved $r_1, r_2, \cdots r_k$ to P_3. Consider $P(x_{g+2}, y_{g+2} \to z_{g+2})$, $P(x_{g+3}, y_{g+3} \to z_{g+3})$, $\cdots$, $P(x_{g+h+1}, y_{g+h+1} \to z_{g+h+1})$ in C, which is moving all $r_1, r_2, \cdots r_k$ from P_2 to P_3. This means $h \geq 2^k-1$. On the other hand if the final position of the rings are at P_2, then we have to vacate P_2 and place all $r_1, r_2, \cdots r_k$ to P_1 (which again takes 2^k-1 steps) before placing r_{k+1} on P_2 again, so this takes more than $2^k-1+1 = 2^k > 2^k-1$ steps. Therefore, the total number of steps is $g+h+1 \geq (2^k-1)+(2^k-1)+1 = 2^{k+1}-1$.

Comment. Intuitively, we could have shortened the solution and say that "if we need 2^k-1 steps to move all rings when $n=k$, then we need 2^k-1 steps to move the first k rings to a single other peg when $n=k+1$". However, this does not address a potential (seemingly stupid, but nevertheless legitimate) question that we shall ask: what if the bottom ring r_{k+1} has the superpower and help to speed up the process? Why can't it impede some intermediate process?

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 $\frac{a^n-1}{a-1} = a^{n-1}+a^{n-2}+\cdots a+1 \equiv \underbrace{1+1+\cdots+1}_{n \text{ times}} = n \pmod{x}$. 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 common 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 yields $\gcd(\frac{a^n-1}{a-1}, a-1) = \gcd(a-1, n)$.

2. We claim that $\gcd(n, n+k) = k, \forall k \in [1, 20]$ by inducting on k. Notice that $\gcd(n, n+k)|n$ and $\gcd(n, n+k)|n+k$ so $\gcd(n, n+k)|(n+k)-n = k$. Thus $\gcd(n, n+k) \leq k$. 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 justified 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 $k|n$ and $k|n+k$. This means $3|n, 7|n$ and since $\gcd(3,7) = 1$, lcm(3,7)=$3 \times 7 = 21$ so $21|n$ and $\gcd(n, n+21) = 21 > 20 = \gcd(n, n+20)$.

   Comment. Notice that the problem is true if we replace 21 with any number that is not a prime power. A slightly harder version of this problem is Problem 3 in International Mathematics Tournament of Towns, Senior O-Level:

http://www.math.toronto.edu/oz/turgor/archives/TT2013F_SOsolutions.pdf. Have fun trying!

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 $2^k = 2^{bd+r} = 2^{bd} \cdot 2^r = (2^d)^b \cdot 2^r \equiv 1^b \cdot 2^r = 2^r \pmod{x}$. 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 $x = \gcd(2^a - 1, 2^b - 1) | 2^d - 1 | 2^{\gcd(a,b)} - 1$, 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 $\times$ 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
   $1(1) + 1(2^k - 1) + 2(1) + 2(2^k - 1) + \cdots + 2^{k-1}(1) + (2^{k-1})(2^k - 1)$
   $= (1 + 2^k - 1) + 2(1 + 2^k - 1) + \cdots 2^{k-1}(1 + 2^k - 1)$
   $= (1 + 2 + \cdots 2^{k-1})(1 + 2^k - 1)$
   $= (2^k - 1)(2^k)$
   $= 2(2^{k-1})(2^k - 1)$.

   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 $\gcd(a^n, b^n) = \gcd\left(\left(\prod_{i=1}^{k} p_i^{a_i}\right)^n, \left(\prod_{i=1}^{k} p_i^{b_i}\right)^n\right) = \gcd\left(\prod_{i=1}^{k} p_i^{na_i}, \prod_{i=1}^{k} p_i^{nb_i}\right) = \prod_{i=1}^{k} p_i^{\min(na_i, nb_i)} = \prod_{i=1}^{k} p_i^{n\min(a_i, b_i)} =$

$\left(\prod_{i=1}^{k} p_i^{\min(a_i,b_i)}\right)^n = (\gcd(a,b))^n$. 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. For clarity we denote b_i as the digit appended on the end of a_{i-1} to form a_i. We will use this fact: if $a_i = k = a_j$ for some $k > 0$ then $i = j$ (since a_i and a_j has the same number of digits). We split into several scenarios:
   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 (except possibly when a_i is a single digit number 2, which happens at most once). If b_i is 0 or 5 for infinitely many i then for such i, $5|a_i$, hence composite (except possibly when a_i is a single digit number 5, which happens at most once).

   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 $N \leq c_1 < c_2 < \cdots$ that contains all 1s and 7s. In other words, for all $i \in \mathbb{N}$, we have $b_{c_i} \in \{1,7\}$ (i.e. $b_{c_i} \equiv 1 \pmod 3$) and for all j with $c_x < j < c_{x+1}$ some x, $b_j = 3$. Also let $a_{c_1} \equiv g \pmod 3$ for some $g \in \{0,1,2\}$. Now for all $i \geq 1$, $a_{c_{i+1}} \equiv a_{c_i} + b_{c_i+1} + \cdots + b_{c_{i+1}-1} + b_{c_{i+1}} \equiv a_{c_i} + 3 + 3 + \cdots + 3 + 1 \equiv a_{c_i} + 1$ (we used the fact that for every integer n, n is equal to its sum of digits in modulo 3). Inductively, $a_{c_{i+1}} \equiv a_{c_1} + i \equiv g + i \pmod 3$. Now if $i = 3k - g$ for all $k \geq 1$, $a_{c_{i+1}} \equiv i + g = (3k-g) + g = 3k \equiv 0 \pmod 3$, which is composite (except possibly when $a_i = 3$ for some i, which can occur at most once).

   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 $k \geq N$, hence a_k composite except for at most once a_k with $a_k = 3$. Now let's assume $3 \nmid m$. We can see that $\gcd(10, m) = 1$ since m, which ends with digit 3, is divisible by neither 2 nor 5. Now, by Euler-Fermat 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 $j \geq 1$, $a_{N+j\phi(m)} = a_N(10^{j\phi(m)}) + \frac{10^{j\phi(m)}-1}{3}$ $= m(10^{j\phi(m)}) + \frac{10^{j\phi(m)}-1}{3}$ is divisible by m and greater than m (since $\phi(m) \geq 1$), hence is composite. Q.E.D.

2. We need this identity: For each $k \geq 1$, there exists an odd positive integer c with $3^{2^k} - 1 = c \cdot 2^{k+2}$ (in other words the highest power of 2 that divides $3^{2^k} - 1$ is $k+2$). Let's proceed by inducting on k. If $k = 1$ then $3^{2^1} - 1 = 8 = 2^3 = 1 \cdot 2^{1+2}$. Now suppose that for some $p \geq 1$, $3^{2^p} - 1 = c \cdot 2^{p+2}$ 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, 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 the lemma above 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 $|w|-|z| \leq |z-w|$. Comparing 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 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 $\angle BAC = \angle ACB$. This implies ABC is isoceles with $|BC| = |AB|$, and $\frac{|AB|}{|CA|} = \frac{|CA|}{|BC|}$, or $|CA|^2 = |AB| \cdot |BC| = |AB| \cdot |AB| = |AB|^2$, so $|CA| = |AB| = |BC|$.

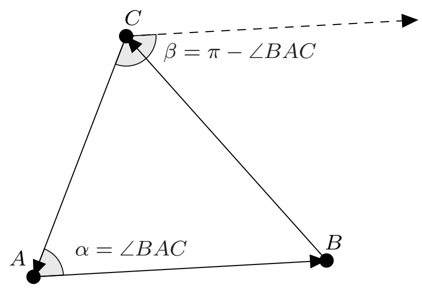

Figure 1: A, B, C in counterclockwise order

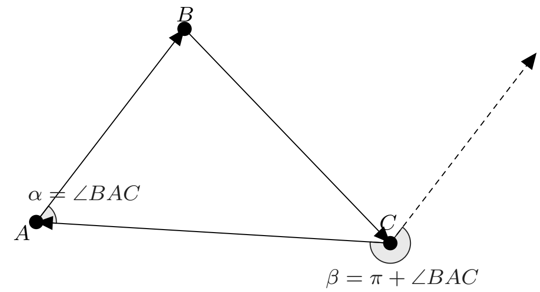

Figure 2: A, B, C are in clockwise order

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.

9 Extra practice 10.

1. Let $\alpha = e^{\frac{2\pi}{5}i}$, then $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ are the roots of $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$. Now write this polynomial as $(x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)$. Now, $(x-\alpha)(x-\alpha^4)$
$= x^2 - (\alpha + \alpha^4)x + \alpha^5$
$= x^2 - (\cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5} + \cos\frac{8\pi}{5} + i\sin\frac{8\pi}{5}) + e^{2\pi}$
$= x^2 - 2\cos\frac{2\pi}{5} + 1$
since $\cos\frac{8\pi}{5} = \cos(2\pi - \frac{2\pi}{5}) = \cos 2\pi \cos\frac{2\pi}{5} + \sin 2\pi \sin\frac{2\pi}{5} = 1 \cdot \cos\frac{2\pi}{5} + 0 \cdot \sin\frac{2\pi}{5} = \cos\frac{2\pi}{5}$ and $\sin\frac{8\pi}{5} = \sin(2\pi - \frac{2\pi}{5}) = \sin 2\pi \cos\frac{2\pi}{5} - \cos 2\pi \sin\frac{2\pi}{5} = 0 \cdot \cos\frac{2\pi}{5} - 1 \cdot \sin\frac{2\pi}{5} = -\sin\frac{2\pi}{5}$. Similarly, $(x-\alpha^2)(x-\alpha^3) = x^2 - 2\cos\frac{4\pi}{5} + 1$. Now we have $x^4 + x^3 + x^2 + x + 1 = (x^2 - 2\cos\frac{2\pi}{5} + 1)(x^2 - 2\cos\frac{4\pi}{5} + 1)$. Equating coefficient of x^3 yield $1 = -2(\cos\frac{2\pi}{5} + \cos\frac{4\pi}{5})$, or $\cos\frac{2\pi}{5} + \cos\frac{4\pi}{5} = \frac{-1}{2}$. Equating the corefficient of x^2 gives $1 = 1 + 1 + (2\cos\frac{2\pi}{5})(2\cos\frac{4\pi}{5}) = 2 + 4\cos\frac{2\pi}{5}\cos\frac{4\pi}{5}$. Thus $\cos\frac{2\pi}{5}\cos\frac{4\pi}{5} = -\frac{1}{4}$. From here we know that $\cos\frac{2\pi}{5}$ and $\cos\frac{4\pi}{5}$ are the roots of the equation $y^2 + \frac{1}{2}y - \frac{1}{4}y = 0$, which gives $y = \dfrac{-\frac{1}{2} \pm \sqrt{(\frac{1}{2})^2 - 4(1)(\frac{-1}{4})}}{2} = \dfrac{-\frac{1}{2} \pm \sqrt{\frac{5}{4}}}{2} = \dfrac{-1 \pm \sqrt{5}}{4}$. Since $\frac{2\pi}{5} < \frac{\pi}{2}$, $\cos\frac{2\pi}{5} > 0$ but as $\frac{-1-\sqrt{5}}{4} < 0$, we have $\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}$.

2. Let $P(x)$ and $Q(x)$ be our primitive polynomials. Let $P(x)Q(x) = c_0 + c_1 x + \cdots + c_n x^n$ for some $n \geq 0$. If $\gcd(c_0, c_1, \cdots c_n) = d > 1$ then d has a prime divisor q and $q|d$. Since $d|c_i$ for all $i \in [1, n]$ we have $q|c_i$ for all $i \in [1, n]$ by transitivity of divisibility. We then have prime

number q dividing all coefficient of $P(x)Q(x)$. Conseuqnetly, if there exists no prime number that divides all coefficient of $P(x)Q(x)$ then $\gcd(c_0, c_1, \cdots c_n) = 1$, and it suffices to show the former (no such prime number).

Now let p be any prime number. Since $P(x)$, $Q(x)$ are both primitive, for each P and Q there exists a coefficient that is not divisible by p. Let $P = a_0 + a_1 x + \cdots + a_k x^k$ and $Q = b_0 + b_1 + \cdots b_m x^m$. Denote i as the least integer with a_i not divisible by p, and denote j as the least integer with b_j not divisible by p (these i, j exist by the least element property). We claim that $p \nmid c_{i+j}$. Indeed, $c_{i+j} = \sum_{r=0}^{i+j} a_r b_{i+j-r}$. For all $r < i$ we have $p | a_r$ by the minimality of i so $p | a_r b_{i+j-r}$. For all $r > i$ we have $i + j - r < i + j - i = j$ so $p | b_{i+j-r}$ by the minimality of j and $p | a_r b_{i+j-r}$ (convince yourself that this claim hold even as $i = 0$ or $j = 0$). Therefore $\sum_{r=0}^{i+j} a_r b_{i+j-r} \equiv a_i b_j \not\equiv 0 \pmod{p}$, since none of a_i and b_j is divisible by p.

Comment: This leads to Gauss's lemma: for any polynomial $P \in \mathbb{Z}[x]$, if there exists $Q, R \in \mathbb{Q}[x]$ with $P = QR$, then there exists $Q', R' \in \mathbb{Z}[x]$ with $P = Q'R'$.