Problem Set 5

1. (a) Four-digit number $S = aabb$ is a square. Find it; (*hint:* 11 *is a factor of* S)
   (b) If n is a sum of two square, so is $2n$. (`Frank`)

   Solution: (a) Since $(A+B)-(A+B)=0$, and $11|0$, $11|AABB$. Thus $11k = AABB$ for some $k \in \mathbf{Z}$. Since $AABB$ is a four digit number and 11 is a two digit number, k must be a three digit number. Let $k = XYZ$, where X, Y and Z are digits. Then:

$$\begin{aligned} AABB &= 11k \\ &= (10+1)k \\ &= (10+1)XYZ \\ &= XYZ0 + XYZ \end{aligned}$$

   So we have:

$$\begin{array}{r} \text{XYZ0} \\ +\ \text{XYZ} \\ \hline \text{AABB} \end{array}$$

   Hence, $Z = B$, $Y = 0$, and $X = A$. Thus $k = XYZ = A0B$. Since $AABB$ is a square, we can write $AABB = m^2$, for some $m \in \mathbf{Z}^+$. Since $AABB = 11(A0B)$, we have $11(A0B) = m^2$, so $11|A0B$. In order for this to be true, we must have $11|A+B$. Since A and B are single digits, their sum must be one of the following:

$$1, 2, 3, ..., 11, 12, 13, 14, 15, 16, 17, 18$$

   Since only one of these is divisible by 11, $A + B = 11$. Thus $A0B$ must be one of the following:

$$209, 308, 407, 506, 605, 704, 803, 902$$

   Dividing each of these by 11, we have:

$$19, 28, 37, 46, 55, 64, 73, 82$$

   Since $AABB = 11(A0B)$ is a perfect square, $A0B/11$ must be a perfect square. Only one of the above is a perfect square: 64. Hence, A0B=704. Therefore AABB=7744.

   (b) If n is the sum of two squares, so is $2n$

   Proof: Consider the following lemma.

   Lemma: The set S_2, consisting of the sums of two squares, is closed under multiplication.

Proof: Let $s = a_1^2 + b_1^2$ and $t = a_2^2 + b_2^2$ be elements of S_2, where $a_1,\ b_1, a_2, b_2 \in \mathbf{Z}$. Then:

$$\begin{aligned} st &= (a_1^2 + b_1^2)(a_2^2 + b_2^2) \\ &= a_1^2a_2^2 + b_1^2a_2^2 + a_1^2b_2^2 + b_1^2b_2^2 \\ &= (a_1^2a_2^2 - 2a_1a_2b_1b_2 + b_1^2b_2^2) + (a_1^2b_2^2 + 2a_1a_2b_1b_2 + b_1^2a_2^2) \\ &= (a_1a_2 - b_1b_2)^2 + (a_1b_2 + b_1a_2)^2 \end{aligned}$$

Since n is a sum of squares, let $n = k^2 + m^2$. Since $2 = 1^2 + 1^2$, we have $2n = (1^2 + 1^2)(k^2 + m^2)$. Since $2n$ can be expressed as the product of two sums of squares, by the above lemma, $2n$ is a sum of squares.

2. (a) If n is an even number, then $323|20^n + 16^n - 3^n - 1$; (*hint: factorize* 323)
(b) If n is an integer, then $9|4^n + 15n - 1$. (*hint: consider cases when* n *modulus* 3)
(`Ben`)

Solution. (a) The first thing to note on this problem is that 323 can be factored, that is $323 = 17 \cdot 19$.

Now from number theory we know that if two numbers are relatively prime, and they each individually divide a sum or difference, then their product divides the sum or difference. And $gcd(17, 19) = 1$, that is, they are relatively prime. Thus it is enough to show that 17 and 19 individually divide

$$20^n + 16^n - 3^n - 1. \tag{1}$$

First we will show that 17 divides (1). Now

$$20^n \equiv 3^n\,(mod 17)\ \ and\ \ 16^n \equiv (-1)^n\,(mod 17)$$

And so

$$20^n + 16^n - 3^n - 1 \equiv 3^n + (-1)^n - 3^n - 1 = 0\,(mod 17),$$

since n is an even number. That is, $17 \mid 20^n + 16^n - 3^n - 1$.

Now, to show 19 divides (1), observe that

$$20^n \equiv 1^n\,(mod 19)\ \ and\ \ 16^n \equiv (-3)^n\,(mod 19)$$

And so

$$20^n + 16^n - 3^n - 1 \equiv 1^n + (-3)^n - 3^n - 1 = 0\,(mod 19),$$

since n is an even number. That is, $19 \mid 20^n + 16^n - 3^n - 1$.

(b) For this problem, it is easiest to proceed by induction. First, observe that

$$9 \mid 4^n + 15n - 1$$

holds for the case $n = 1$, because $9 \mid 18$.

A fact that will be used later (which comes from Number Theory) is the following: If $a \mid b$ and $a \mid c$, then we can conclude that $a \mid b \pm c$. Also, knowing any two of the statements to be true is enough to conclude the third.

Now assume that $9 \mid 4^n + 15n - 1$. We will show that $9 \mid 4^{n+1} + 15(n+1) - 1$.

Using the fact from above, it is equivalent to show that

$$9 \mid [4^{n+1} + 15(n+1) - 1] - [4^n + 15n - 1].$$

Now, expanding, grouping and simplifying terms, we find

$$\begin{aligned}
[4^{n+1} + 15(n+1) - 1] - [4^n + 15n - 1] &= 4^{n+1} + 15n + 15 - 1 - 4^n - 15n + 1 \\
&= [4^{n+1} + 4^n] + [15n - 15n] + [1 - 1] + 15 \\
&= 4^n(4 - 1) + 15 \\
&= 3 \cdot 4^n + 3 \cdot 5 \\
&= 3(4^n + 5)
\end{aligned}$$

Noting that $4^n \equiv 1^n = 1\,(mod 3)$ and that $5 \equiv 2\,(mod 3)$ yields

$$\begin{aligned}
3(4^n + 5) &\equiv 3(1 + 2)\,(mod 3) \\
&= 3(3) \\
&= 9
\end{aligned}$$

Thus $9 \mid [4^{n+1} + 15(n+1) - 1] - [4^n + 15n - 1]$ as wanted, and so we can conclude that $9 \mid 4^{n+1} + 15(n+1) - 1$, and finally that $9 \mid 4^n + 15n - 1$.

3. (a) If $2n + 1$ and $3n + 1$ are squares, then $5n + 3$ is not a prime; (*hint: express* $5n + 3$ *by* $2n + 1$ *and* $3n + 1$)
(b) If $3n + 1$ and $4n + 1$ are squares, then $56|n$. (*hint: follow the idea in presentation problem*) (`Beth`)

Since both $2n + 1$ and $3n + 1$ are squares, let 2n+1 = a^2, and let 3n+1 = b^2.

$5n + 3 = 4(2n + 1) - (3n + 1)$

so 5n+3 = $4(a^2)$ - (b^2)

$5n + 1 = (2a)^2 - (b^2)$

notice this is a difference of squares, so $5n + 3 = (2a - b)(2a + b)$.

Thus $5n + 3$ is NOT prime.

B. Prove: If 3n+1 and 4n+1 are squares, then 56—n.

If we can prove that 8 divides n, and 7 divides n, then we know that 56 divides n.

Let 4n+1 = b^2, and let 3n+1 = a^2.

Then n = $b^2 - a^2$.

We know that 4n+1 is odd $\Rightarrow$ so b^2 is odd.

Let's assume that n is odd. Therefore, n=2m+1. Then we have that $b^2 = 8m + 5$.

If we make a table of b, and b^2 mod 8, then we get:

b	0	1	2	3	4	5	6	7
b^2	0	1	4	1	0	1	4	1

and we don't ever get 5 mod 8. Therefore n is even.

Thus we have that a^2 is odd, and a is odd. From there we get that (b-a)(b+a) are both even, and then n is divisible by 4.

So b and a are either equivalent to 1 or 3 mod 4. There are four cases:

a	1	1	3	3
b	1	3	1	3
$(b-a)(b+a)$	$0*2$	$2*0$	$-2*0$	$0*2$

Thus 8—n.

The case for 7 is much more difficult. It involves using Pell's equation to find a solution.

Theorem: (x_1, y_1) is the smallest solution for $x^2 - Dy^2 = 1$, then $x_k + \sqrt{D}y_k = (x_1 + \sqrt{D}y_1)^k = (x - \sqrt{D}y)^k(x + \sqrt{D}y)^k$ is also a solution.

So, in our problem, if you set $4n + 1 = b^2$, and $3n + 1 = a^2$ and multiply the first equation by 4, and the second by 3, you get:

$4a^2$ - $3b^2 = 1$

x=2a, y=b so x^2 -$3y^2 = 1$.

Solving this equation with Pell's equation, then the first two answers you get are (2,1) and (7,4) and this second one shows that n is divisible by 7.

4. (a) If p is a prime, then $p^2 \equiv 1(mod 24)$; (*hint: prove* $24|p^2 - 1$)
(b) Show that if n divides a single Fibonacci number, then it will divide infinitely many Fibonacci numbers. (*hint: think Problem Set 2 number 10.*) (`Tina`)

Solution:
This is only true for primes ≥ 5, and from this point all primes are odd.

$$p^2 \equiv 1(\text{mod } 24) \implies \begin{array}{l} 24|(p^2-1) \\ 24|(p-1)(p+1) \end{array}$$

Since p is odd, both $(p-1)$ and $(p+1)$ are even and therefore divisible by two. Furthermore, since $p \equiv \pm 1$ (mod 4), either $(p-1)$ or $(p+1)$ is divisible by 4. Finally, as is true for all prime numbers, $p \equiv \pm 1$ (mod 3), and therefore, either $(p-1)$ or $(p+1)$ is divisible by 3. So combining all of these facts, $(p-1)$ or $(p+1)$ is divisible by 4, the other is divisibly by 2, and one is divisible by 3. $(4)(2)(3) = 24$ and therefore $p^2 \equiv 1$ (mod 24).

4b) Show that if n divides a single Fibonacci number, then it will divide infinitely many Fibonacci numbers.

Solution:
Write the Fibonacci numbers $F_1, F_2, F3, ...$ in the following form:

$$(a_1, a_2), (a_3, a_4), (a_5, a_6)...$$

where $a_k = F_k (\text{mod } n)$. Obviously, the series will begin (1,1). At some point in this series, (a_i, a_{i+1}) will equal (a_j, a_{j+1}). Since the Fibonacci numbers are cyclical, every a_i is completely determined by a_{i-2} and a_{i_1}. Therefore, the only way to get (1,1) is if the second number in the pair immediately before it is zero (in other words, divisible by n). So once we find a pair that repeats, it will repeat an infinite number of times, and during each cycle there will be at least one number that is divisible by n.

5. (a) (VT 1979) Show that for all positive integers n, that 14 divides $3^{4n+2} + 5^{2n+1}$;
(b) (VT 1981) $2^{48} - 1$ is exactly divisible by what two numbers between 60 and 70?
(*hint: (a)* $14 = 2 \cdot 7$*, (b) factorizing*) (`Lei`)

Solution. (a) We can rewrite

$$3^{4n+2} + 5^{2n+1} \equiv 3^2 * 3^{4^n} + 5 * 5^{2^n} \equiv 9 * 81^n + 5 * 25^n \equiv 9 * (-3)^n + 5 * (-3)^n$$

$$mod(14)$$

Which is obviously divisble by 14.

(b) Since

$$(\pm 1)^k - 1 \equiv 0$$

if k is even. We can start by rewriting

$$2^4 8 - 1 = 2^{6*8} - 1$$

Since $2^6 = 64$ and $64 \equiv \pm 1$ mod 65 and 63. So $2^{48} - 1$ is divisible by 65 and 63.

6. (a) (VT 1982) What is the remainder when $X^{1982} + 1$ is divided by $X - 1$? Verify your answer (*hint: too simple*);
(b) (MIT training 2 star) Let n be an integer greater than one. Show that $n^4 + 4^n$ is not prime. (*hint: there is a magic identity due to Sophie Germain:* $a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$) (`Erin`)

a) It is pretty easy to see that the answer is 2. Simply do direct long division to obtain the answer. b) We are trying to show that $n^4 + 4^n$ is not prime. The first thing to do is note that if n is even we are done. Secondly, since we have the 'magic identity' which says that $a^4 + 4b^n = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$ we simply need to match up the two equations. Let $a = n$, this takes care of the first term. Let $4^n = 4b^4 \implies 4^{n-1} = b^4 \implies 2^{n-1} = b^2 \implies 2^{2m} = b^2$ (since n is odd) $\implies 2^m = b$ and we are done.

7. (VT 1988) Let a be a positive integer. Find all positive integers n such that $b = a^n$ satisfying the condition that a^2+b^2 is divisible by $ab+1$. (*hint: prove that* $a^m+1|a^n+1$, *then* $m|n$.) (`Brett`)

   Solution. We need to find all positive integers n such that $(a^2+a^{2n})/(a^{n+1}+1) \in \mathbf{N}$. Rewrite this to get,

$$\begin{aligned} \frac{a^2(1+a^{2n-2})}{a^{n+1}+1} \in \mathbf{N} &\Rightarrow (a^{n+1}+1)|(a^{2n-2}+1) \\ &\Rightarrow (n+1)|(2n-2) \\ &\Rightarrow n = (m+2)/(2-m) \text{ for some } m \in \mathbf{Z} \end{aligned}$$

   This gives possible n values of 0, 1, or 3.
   0 and 1 both fail for $a = 2$. However, $n = 3$ gives a result of $a^2 \in \mathbf{N}$ for all values of a. So n must be equal to 3.

8. (Putnam 1972-A5) Show that if n is an integer greater than 1, then n does not divide $2^n - 1$. (`Shelley`)

   Solution:

   Assume the opposite: $2^{n-1} \vdots 1 \pmod{p}$, n = odd because 2^n is even . Take p such that it is the smallest prime dividing n, and m is the smallest divisor of p-1. Then $2^{n-1} \vdots 1 \pmod{p}$ is equivalent to $2^m \equiv 1\ (modp)$, for $m < p$.

   m must be co-prime to n, because p is the smallest prime divisor. So, $n = xm+r, 0 < r < m$. It follows that $2^r \equiv 1(modp)$. However, m is the smallest divisor of $p-1$. Contradiction.

9. (Putnam 1986-A2) What is the units (*i.e.*, rightmost) digit of $\left[\dfrac{10^{20000}}{10^{100}+3}\right]$? Here $[x]$ is the greatest integer $\leq x$. (`Richard`)

   Solution. First note $20000/100 = 200$, which is the ratio of the numerator to the dominator. Now consider the factorization $x^{200} - y^{200} = (x-y) * (x^{199} + x^{198} * y + ... + y^{199})$

   Taking $x = 10^{100}$ and $y = -3$ in the above factorization shows that the number $A = (10^{20000} - 3^{200})/(10^{100}+3)$ is an integer. Moreover, $(10^{20000} - 3^{200})/(10^{100}+3) = [10^{20000}/(10^{100}+3)]$, since $3^{200}/(10^{100}+3) = 9^{100}/(10^{100}+3) < 1$ So A is congruent to -3^{199} which is congruent to 3 mod 10. Hence, the units digit is 3.

10. (Putnam 1998-A4) Let $A_1 = 0$ and $A_2 = 1$. For $n > 2$, the number A_n is defined by concatenating the decimal expansions of A_{n-1} and A_{n-2} from left to right. For example $A_3 = A_2A_1 = 10$, $A_4 = A_3A_2 = 101$, $A_5 = A_4A_3 = 10110$, and so forth. Determine all n such that 11 divides A_n. (`David Rose`)

    Solution We first define $\phi(n)$ as the number of digits in A_n. Simple induction shows that $\phi(n)$ is odd if $n \equiv 1, 2(mod3)$ and even if $n \equiv 0(mod3)$. Now note that the definition of A_n is equivalent to $A_n = 10^{\phi(n-1)}A_{n-1} + A_{n-2}$. Now, noting that $10 \equiv -1(mod11)$ we see that $A_n \equiv (-1)^{\phi(n-1)}A_{n-1} + A_{n-2}(mod11)$. Now, we claim that

$$
\begin{aligned}
n \equiv 1 (mod 6) &\Rightarrow A_n \equiv 0 (mod 11) \\
n \equiv 2 (mod 6) &\Rightarrow A_n \equiv 1 (mod 11) \\
n \equiv 3 (mod 6) &\Rightarrow A_n \equiv -1 (mod 11) \\
n \equiv 4 (mod 6) &\Rightarrow A_n \equiv 2 (mod 11) \\
n \equiv 5 (mod 6) &\Rightarrow A_n \equiv 1 (mod 11) \\
n \equiv 0 (mod 6) &\Rightarrow A_n \equiv 1 (mod 11)
\end{aligned}
$$

We will verify using induction. We can check that these hold for $n = 1, 2, 3, 4, 5, 6$ using our formula above. With this base, we can use circular induction to show that these statements hold for all n. For example, assume the above holds for $n \equiv 1 (mod 6)$ and $n + 1 \equiv 2 (mod 6)$. Then $A_{n+2} \equiv (-1)^{odd}(1) + 0 = -1$. The rest of the induction follows similarly.