UT Putnam Prep Problems, Nov 2, 2016 (Go, Cubbies, Go!)
NUMBER-THEORY PUTNAM PROBLEMS

1. Find all positive integers that are within 250 of exactly 15 perfect squares. (Note: A *perfect square* is the square of an integer; that is, a member of the set $\{0, 1, 4, 9, 16, \ldots\}$. We say "$a$ is within n of b" if $b - n \leq a \leq b + n$.)

ANSWER: The question is about the number of perfect squares in the interval $[b-T, b+T]$ where $T = 250$. If the largest perfect square to the left of this interval is n^2, then the interval will include precisely the k squares $(n+1)^2, \ldots, (n+k)^2$ where k is the largest integer for which $(n+k)^2 \leq b+T$. Note that we then have inequalities $n^2 < b-T \leq (n+1)^2$ and $(n+k)^2 \leq b+T < (n+k+1)^2$ and in fact the unique integer k consistent with these inequalities determines the number of squares in the interval. Adding the 1st and 4th inequalities, or the 2nd and 3rd, show that

$$2T < 2n(k+1) + (k+1)^2, \qquad 2n(k-1) + (k^2-1) \leq 2T$$

(after a bit of simplifying) from which we deduce that

$$T/(k+1) - (k+1)/2 < n \leq T/(k-1) - (k+1)/2$$

So for example we were given parameters $T = 250$ and $k = 15$ and thus discover that $n = 8$ is the only integer that will work: the fiften squares must be $9^2 = 81, 10^2, \ldots, 23^2 = 529$, and then the defining conditions on b are: $64 < b - 250 \leq 81$ and $529 \leq b + 250 < 576$, i.e. we must have $b > 314$, $b \leq 331$, $b \geq 279$, and $b < 326$. So it seems to me the integers in question are the eleven numbers $b = 315, 316, \ldots, 325$.

2. Find the smallest positive integer n such that for every integer m, with $0 < m < 1993$, there exists an integer k for which

$$\frac{m}{1993} < \frac{k}{n} < \frac{m+1}{1994}$$

ANSWER: It seems to be not as widely known as I thought that if a, b, c, d are all positive then $(a+c)/(b+d)$ lies between a/b and c/d. So certainly one solution is to have $n = 1993 + 1994$ (with $k = 2m+1$). To see that no smaller n will do, let's see what the k would have to be in the case $m = 1992$. By hypothesis there is an integer k with $1 - 1/1993 < k/n < 1 - 1/1994$; writing $k = n - j$ we discover j must be a (positive) integer with $n/1993 > j > n/1994$. If indeed we could do this with an $n < 3987$, then the left side would be at most 2, in which case we would need $j = 1$ and then the inequalities require $1993 < n < 1994$, which cannot be true for integers n. Thus we must indeed have $n \geq 3987$.

3. How many primes among the positive integers, written as usual in base 10, are such that their digits are alternating 1s and 0s, beginning and ending with 1?

ANSWER: How many 1s are in the decimal expansion of this number N? If there are k of them, then, $99N$ is a string of $2k$ 9's, i.e. $99N = 10^{2k} - 1 = (10^k - 1)(10^k + 1)$. Now since $10 \equiv -1 (\bmod 11)$ we see 11 divides either the left or the right factor depending on whether k is even or odd; and certainly 9 divides the first factor (since $10 \equiv +1 \bmod 9$). So depending on the parity of k we have a factorization of N into integers, either

$$(10^k - 1)/99) \cdot (10^k + 1) \qquad \text{or} \qquad ((10^k - 1)/9) \cdot ((10^k + 1)/11)$$

These factors are clearly greater than 1 for $k > 2$. So the lone prime in this sequence is $N = 101$.

4. A *composite* (positive integer) is a product ab with a and b not necessarily distinct integers in $\{2, 3, 4, \ldots\}$. Show that every composite is expressible as $xy + xz + yz + 1$, with x, y, and z positive integers.

ANSWER: One solution is simply to take $x = 1, y = a - 1, z = b - 1$ or some permuation thereof. There must be other answers because for example when $a = 5, b = 11$ I also find solutions $\{x, y, z\} = \{3, 4, 6\}$; when $a = 7, b = 13$ I also find $\{x, y, z\} = \{3, 6, 8\}$; etc. Please let me know if you discover another pattern.

5. For a given positive integer m, find all triples (n, x, y) of positive integers, with n relatively prime to m, which satisfy $(x^2 + y^2)^m = (xy)^n$.

ANSWER: If p is a prime dividing x, then it divides the right side, hence the left side, hence y^{2m}, hence y itself. More generally it's not hard to check that y is divisible by whatever power of p divides x. Since this is true for all p, x itself divides y. Similarly $y|x$, so x and y are equal, and our equation just states that $(2x^2)^m = x^{2n}$, and thus $2^m = x^{2n-2m}$. So x is a power of 2, say $x = 2^r$, and $m = 2r(n - m)$, or $(2r + 1)m = 2r(n)$. Since m and n are given as coprime, and $2r$ and $2r + 1$ obviously are as well, we deduce $n = 2r + 1$, $m = 2r$, and $x = y = 2^r$. Taking $r = 0, 1, 2, \ldots$ gives all the solutions (x, y, m, n). (In particular, there are NO solutions with m odd.)

6. Prove that, for any integers a, b, c there exists a positive integer n such that

$$\sqrt{n^3 + an^2 + bn + c}$$

is not an integer.

ANSWER: We have to show there is a positive integer n for which $p(n) = n^3 + an^2 + bn + c$ is not an perfect square. In fact I claim that one of $n = 1, 2, 3, 4$ will do! For if each of these values of $p(n)$ is a perfect square, then each is congruent to either 0 or 1 modulo 4. In that case, differences like $p(3) - p(1)$ and $p(4) - p(2)$ cannot be congruent to 2 mod 4. On the other hand, when we do compute these modulo 4, we get $p(3) - p(1) \equiv 2 + 2b$ and $p(4) - p(2) \equiv 2b$; both of these are obviously even so if they're not congruent to 2 mod 4, they must each be multiples of 4, and that's not possible since they differ by 2 (mod 4).

This simple solution is adapted from one presented by a student. There's a lot of deep theory that seems like it can be applied here too, but I think that mostly obscures rather than illuminates. Equations of the form $y^2 = p(x)$ generally describe curves known as *elliptic curves* when p is a cubic polynomial, and the problem of finding points (x, y) on a curve whose coordinates are integers (or rational numbers) is called a *Diophantine problem*. In the particular example of elliptic curves it is known that there can only be finitely many integer points on such a curve. (Also, while there may be infinitely many rational points on such a curve, the collection of them all is "not too big" – they form a finitely-generated abelian group, about which quite a bit is known (and some important things are unknown!). The Diophantine analysis of elliptic curves lay at the heart of the solution to Fermat's Last Theorem, for example.) That said, it is worth point out that for some combinations of a, b, c (for example $a = b = c = 0$) this is not actually an elliptic curve, and may indeed have infinitely many integer points. So to summarize: don't let the advanced stuff stand in the way of getting a quick answer!

7. Let N be the positive integer with 2016 decimal digits, all of them being 1, that is, $N = 111\ldots111$ (2016 digits). Find the thousandth digit after the decimal point of $\sqrt{N}$.

ANSWER: Note that $9N+1 = 10^{2016}$ so that $3\sqrt{N} = \sqrt{10^{2016} - 1} = 10^{1008}\sqrt{1-\epsilon}$ where $\epsilon = 10^{-2016}$. Using the Binomial Theorem we can expand $(1-\epsilon)^{1/2} = 1 - \epsilon/2 - \epsilon^2/8 + \ldots$, which is actually the Taylor Series. We can use Taylor's Theorem (with Remainder) to be more precise but clearly for small ϵ this differs from $1 - \epsilon/2$ by less than ϵ^2. So in our case, $3\sqrt{N} = 10^{1008} - 10^{-1008}/2 - \delta$ where the last factor δ is smaller than 10^{-3024}. So the first 3024 or so digits of $\sqrt{N}$ agree with $(10^{1008} - 1)/3 + (1/3) - (10^{-1008}/6)$, which has has 1008 3's to the left of the decimal point, then a string of 3's after the decimal point that is unbroken until the 1009th digit, where we find a 1 followed by a couple thousand 6's.

The corresponding question was just a tad harder before the year 2000!

8. Let S be a finite set of integers, each greater than 1. Suppose that for each integer n there is some $s \in S$ such that either $\gcd(s, n) = 1$ or $\gcd(s, n) = s$. Show that there exists $s, t \in S$ such that $\gcd(s, t)$ is prime. [Here $\gcd(a, b)$ denotes the greatest common divisor of a and b.]

ANSWER:

9. Show that no four consecutive binomial coefficients can lie in an arithmetic progression:

$$\binom{n}{r}, \quad \binom{n}{r+1}, \quad \binom{n}{r+2}, \quad \binom{n}{r+3}$$

ANSWER: We may write each of these four terms as a multiple of $n!/(r+3)!(n-r)!$, the multipliers being respectively

$$(r+3)(r+2)(r+1),\ (r+3)(r+2)(n-r),\ (r+3)(n-r)(n-r-1),\ (n-r)(n-r-1)(n-r-2)$$

The original four terms are in progression iff these are, and that happens iff the consecutive differences are equal. So the conditions that n and r must satisfy to give an arithmetic progression are that

$$\begin{aligned}(r+3)(r+2)(r+1) &- (r+3)(r+2)(n-r)\\ &= (r+3)(r+2)(n-r) - (r+3)(n-r)(n-r-1)\\ &= (r+3)(n-r)(n-r-1) - (n-r)(n-r-1)(n-r-2)\end{aligned}$$

That's two equations in two unknowns so there's reason to expect a small number of solutions. In fact after a bit of slogging the solutions to these polynomial equations turn out to be only the six integer points with $-3 \leq r \leq n \leq -1$, and in particular none of them have $n > 0$,

(It is perhaps appropriate to observe that I have assumed the binomial coefficients can be expressed as products of factorials and in particular are nonzero, i.e. that $0 \leq r \leq n-3$; otherwise there *are* long arithmetic progressions of binomial coefficients, such as $\binom{5}{7}, \binom{5}{8}, \binom{5}{9}, \binom{5}{10}, \ldots$, all of them being zeros of course.)