1(a). Write 2005 in base 17.

The algorithm is to perform a series of divisions with remainder:

\[
\begin{align*}
2005/17 &= 117, \text{ remainder } 16; \\
117/17 &= 6, \text{ remainder } 15; \\
6/17 &= 0, \text{ remainder } 6.
\end{align*}
\]

The conclusion is that the base 17 representation of 2005 is

\[(6)(15)(16) = 6 \cdot 17^2 + 15 \cdot 17 + 16.\]

1(b). What was the most recent year divisible by 17?

To get the most recent year divisible by 10, you drop the last digit from 2005, leaving 2000. To get the most recent year divisible by 17, you drop the one’s place from the base 17 representation, leaving

\[(6)(15)(0) = 6 \cdot 17^2 + 15 \cdot 17 = 6 \cdot 289 + 15 \cdot 17 = 1734 + 255 = 1989.\]

The most recent year was 1989.

1(c). What was the most recent year divisible by 289?

This time you drop the one’s place and the 17’s place, leaving

\[(6)(0)(0) = 6 \cdot 17^2 = 1734.\]

It’s been a while.

2. Division with remainder works for dividing by any positive integer, including 1. Explain why this does not lead to a “base 1” representation of any positive integer as a string of zeros.

In the algorithm for expanding a natural number \( n \) in base \( b \), you use division with remainder to write \( n = ab + r \), with \( 0 \leq r < b \). In the algorithm for finding the base \( b \) expansion, you repeat this process, replacing \( n \) by \( a \), and continue until \( a = 0 \). The reason this works is that for \( b > 1 \), necessarily

\[a = (n - r)/b \leq n/b < n\]

for any \( n > 1 \). So you’re getting strictly smaller natural numbers (or zero, when you stop); so the process has to end. When \( b \) is equal to 1, division with remainder just gives \( n = n \cdot 1 + 0 \): the remainder is always zero, and the next number \( a \) is always equal to \( n \). So the process never terminates.

Actually there is a variant of division with remainder in which you allow remainders of 1, 2, \ldots, \( b \). The statement that it works is

**Proposition.** Suppose that \( b \) is a natural number and \( n \) is any integer. Then there are unique integers \( a' \) and \( r' \) satisfying

\[n = a'b + r', \quad 1 \leq r' \leq b.\]

If \( n > 0 \), then \( a' \) is non-negative, and \( a' < n \).
If you use this variant, then the successive “quotients” $a'_{j}$ get strictly smaller until they get to 0. (When you divide 0 by $b$, the “quotient” is $-1$ with a “remainder” of $b$.) This algorithm produces a kind of “base $b$” representation of each natural number $n$ in which the “$b^{k}$ place” is occupied by a digit between 1 and $b$ (instead of between 0 and $b - 1$). If we write $X$ for the base 10 digit for ten, then the new representations of some numbers are

$$
\text{old 59 = new 59, old 90 = new 8X, old 305108 = new 2X4X8.}
$$

You may wish to figure out an easy rule for converting between the two representations.

At any rate, in the new representation base 1 makes perfect sense: every natural number $n$ is represented by a string of $n$ ones. The reason is that the variant division by one with remainder always writes $n = (n - 1) \cdot 1 + 1$.

The remainders are always one, so you keep writing them down until you get to a “quotient” of zero.

3. A Pythagorean triple consists of three integers $x$, $y$, and $z$ such that $x^2 + y^2 = z^2$. The triple is called primitive if $x$, $y$, and $z$ have no common prime factor. (So $(3, 4, 5)$ is primitive, but $(18, 24, 30)$ is not.) Euclid showed that if $(x, y, z)$ is a primitive Pythagorean triple, then there are integers $u$ and $v$ so that

$$
\{x, y\} = \{u^2 - v^2, 2uv\}.
$$

Find $u$ and $v$ for the Pythagorean triple $(65, 72, 97)$. (It’s possible to proceed by pure guesswork; or you can do some thinking to direct your guessing; or you can analyze section 1.7 of the text to see how to write down $u$ and $v$ immediately.)

You are asked to find integers $u$ and $v$ so that

$$
u^2 - v^2 = 65, \quad 2uv = 72.
$$

(Euclid’s result doesn’t say which order the pair is in; but since 65 is odd, it can’t be of the form $2uv$.) The medium-clever way to proceed is to factor these equations as

$$(u - v)(u + v) = 5 \cdot 13, \quad uv = 2 \cdot 3 \cdot 3 \cdot 3.$$

The first equation can be solved in only a few ways (because of uniqueness of prime factorization):

$$
u - v = 1, u + v = 65; \quad u - v = 5, u + v = 13; \quad u - v = -5, u + v = -13,
$$

and so on. From each of these possibilities you get two simultaneous linear equations for $u$ and $v$, which are easy to solve; then you can check whether the solution satisfies the second requirement $2uv = 72$. In this way you come pretty quickly to $u = 9, v = 4$ as a solution.

Here’s the more sophisticated solution. From looking at section 7 of the text, you see that $v/u$ is supposed to be the slope of the line through the points $(65/97, 72/97)$ and $(-1, 0)$. This slope is

$$
(72/97)/(1 + (65/97)) = 72/162 = 36/81 = 4/9.
$$

This suggests $u = 4, \ v = 9$. (If you inadvertently used the point $(72/97, 65/97)$, the slope would turn out to be $5/13$, giving $v = 5, u = 13$. Euclid’s formula for this $u$ and $v$ gives the Pythagorean triple $(130, 144, 194)$, which is just twice the one we want.)
4(a). Write down the equation of the tangent line at the point (5, 11) to the curve $y^2 = x^3 - 4$.

Implicit differentiation gives $2y \frac{dy}{dx} = 3x^2$, so at our point $22 \frac{dy}{dx} = 75, \quad \frac{dy}{dx} = 75/22$.
The equation of the tangent line is therefore $y = (75/22)x - (133/22)$; the constant comes from requiring the line to pass through (5, 11).

4(b). Find a rational solution of the equation $y^2 = x^3 - 4$ other than (5, 11). (One possible hint would be to look at the problems in the text for section 1.7, but I gave another hint in class Wednesday.)

The first hint suggests that you look for a point of intersection of the tangent line with the curve. Plugging the equation of the tangent line into the equation of the curve gives

$$(1/22^2)(75x - 133)^2 = x^3 - 4, \quad (1)$$
or

$$x^3 - \frac{75^2}{22^2}x^2 + \frac{150 \cdot 133}{22^2}x - \frac{133^2}{22^2} - 4 = 0. \quad (2)$$

This is a cubic equation in $x$. It turns out to have a double root at $x = 5$; that’s essentially what it means for the straight line to be tangent to the curve there. In other words, this cubic polynomial is divisible by $x^2 - 10x + 25$. Carrying out the division is a fairly painful process, although you ought to be able to manage it. Here is a trick to do it. As I said, we know that the cubic is exactly divisible by $x^2 - 10x + 25$. So let’s carry out the division on the two sides of (1) separately. On the left side, it’s clear that we get

$$[(1/22^2)(75x - 133)^2] \div [x^2 - 10x + 25] = (75/22)^2, \quad \text{with a linear remainder } ax + b.$$  

On the right side of (1) we can carry out the division more explicitly, getting

$$[x^3 - 4] \div [x^2 - 10x + 25] = x + 10, \quad \text{with a linear remainder } 75x - 254.$$  
Since we know that our cubic polynomial is exactly divisible by $(x - 5)^2$, the two linear remainder terms must be the same. The conclusion is that

$$[\text{cubic equation } (2)] \div (x - 5)^2 = x - [(75/22)^2 - 10].$$  
The constant term in this linear equation is $-785/484$. The conclusion is that $x = 785/484$ (and $y$ given by the tangent line equation, or $y = 5497/10648$) is a rational point on the curve $y^2 = x^3 - 4$.

The second hint refers to my statement that I don’t like problems with messy answers (clearly a lie, in light of the preceding paragraph). But the problem didn’t require you to use part (a) to solve part (b); you can just try to find solutions of $y^2 = x^3 - 4$ by pure thinking, or by trial and error. In this case a little trial leads to $x = 2, y = \pm 2$, which is a perfectly acceptable answer to (b).