Math 2710 (Roby) **Practice Midterm #2** Spring 2013

1. Give a careful proof by induction that for every positive integer n

$$1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}$$

For the base case $n = 1$ we get LHS$=1^2 = 1$ and RHS$=\dfrac{1(1)(3)}{3} = 1$, so the equation holds.

Now suppose the equation holds for some $k \in \mathbb{Z}^+$, i.e.,

$$1^2 + 3^2 + 5^2 + \cdots + (2k-1)^2 = \frac{k(2k-1)(2k+1)}{3}$$

We want to show it holds also for $k+1$. We have

$$\begin{aligned}
1^2 + 3^2 + 5^2 + \cdots + (2k+1)^2 &= 1^2 + 3^2 + 5^2 + \cdots + (2k-1)^2 + (2k+1)^2 \\
&= \frac{k(2k-1)(2k+1)}{3} + (2k+1)^2 \\
&= \frac{k(2k-1)(2k+1) + 3(2k+1)^2}{3} \\
&= \frac{(2k+1)[k(2k-1) + 3(2k+1)]}{3} \\
&= \frac{(2k+1)[2k^2 - 5k + 3]}{3} \\
&= \frac{(2k+1)[(k+1)(2k+3)]}{3} \\
&= \frac{(k+1)(2k+1)(2k+3)}{3}
\end{aligned}$$

where the first second equality uses the induction hypothesis. Hence, the equation also holds for $k+1$. So by the Principle of Mathematical Induction, the equation holds for every $n \in \mathbb{Z}^+$.

2. **PODASIP:** For any odd positive integer m, the number of nonzero perfect squares in $\mathbb{Z}_m$ is $\frac{m-1}{2}$.

This is *false*. A counterexample is $n = 9$, where there are three nonzero perfect squares: $1^2 = 1, 2^2 = 4, 4^2 = 7$. (The others are duplicates of these or are zero.) But $\frac{n-1}{2} = 4 \neq 3$.

SALVAGES: (1) True if n is (an odd) prime (Ex. #3.57 from the HW); (2) True in general that the number of nonzero perfect squares is $\leq \frac{n-1}{2}$. (Since $a^2 \equiv (-a)^2 \equiv (n-a)^2 \pmod{n}$.)

3. **PODASIP:** For any $a \in \mathbb{Z}$ and any positive prime p, we have

$$a^{p-1} \equiv 1 \pmod p$$

This is *false*: take $a = 0$, $p = 3$ (or any p). Then $a^{p-1} = 0$ not 1.

SALVAGE: True if $p \nmid a$ (equivalently if $a \not\equiv 0 \pmod p$).

Proof. See your class notes or the text, Theorem 3.42 (Fermat's Little Theorem). ∎

4. (a) State carefully the *definition* of $\varphi(m)$, where m is a positive integer. (Do not give a formula for computing it.)

   $\varphi(m) := \#U_m$, or $\varphi(m) = \{1 \le a \le m : (a, m) = 1\}$.

   (b) Working directly from this definition proof that

$$\varphi(m) = m - 1 \iff m \text{ is prime.}$$

   ($\Leftarrow$) If m is prime, then it has no positive factors besides 1 and itself, for $(a, m) = 1$ for every $1 \le a \le m - 1$. Hence, by definition, $\varphi(m) = m - 1$.

   ($\Rightarrow$) Conversely, if m is not prime, then it has a factorization $m = ab$ where $1 < a, b < m$. For these elements we have $(a, m) = a \neq 1$ and $(b, m) = b \neq 1$, so there are at least two elements strictly between 1 and m which are not relatively prime to m, so by definition $\varphi(m) \le m - 3$.

5. Numerical & Computational problems

   (a) Expand $\left(x + \frac{1}{x}\right)^6$. By the binomial expansion this is

$$x^6 + \binom{6}{1}x^5x^{-1} + \binom{6}{2}x^4x^{-2} + \binom{6}{3}x^3x^{-3} + \binom{6}{4}x^2x^{-4} + \binom{6}{5}x^1x^{-5} + x^{-6}$$
$$= x^6 + 6x^4 + 15x^2 + 20 + \frac{15}{x^2} + \frac{6}{x^4} + \frac{1}{x^6}$$

   (b) Compute $2^{327} \pmod{51}$. We use the Fermat-Euler theorem. Since $51 = 3 \cdot 17$, $\phi(51) = 2 \cdot 16 = 32$. Hence,

$$2^{327} = (2^{32})^{10} \cdot 2^7 \equiv (1)^{10} \cdot 2^7 = 128 \equiv 26 \pmod{51}.$$

(c) Simplify $\dfrac{2\sqrt{3}+3\sqrt{2}}{\sqrt{3}+\sqrt{2}}$.

$$\begin{aligned}\frac{2\sqrt{3}+3\sqrt{2}}{\sqrt{3}+\sqrt{2}} &= \frac{2\sqrt{3}+3\sqrt{2}}{\sqrt{3}+\sqrt{2}}\cdot\frac{\sqrt{3}-\sqrt{2}}{\sqrt{3}-\sqrt{2}} \\ &= \frac{2\cdot 3-2\sqrt{6}+3\sqrt{6}-3\cdot 2}{3-2} \\ &= \sqrt{6}\,.\end{aligned}$$

(d) Compute the following (without a calculator!):

$$9^7+7\cdot 9^6+21\cdot 9^5+35\cdot 9^4+35\cdot 9^3+21\cdot 9^2+7\cdot 9$$

By the binomial theorem, this is $(9+1)^7-1=10^7-1=9,999,999$.

6. **True/False & Explain:** For each statement below, state whether it is true or false and give a convincing reason.

(a) $\sqrt{3}+\sqrt{27}-\sqrt{48}$ is irrational.
False, since it equals $\sqrt{3}+3\sqrt{3}-4\sqrt{3}=0$.

(b) The sum of a rational number and an irrational number is irrational.
True. Let $r\in\mathbb{Q}$ and t be irrational. Suppose BWOC that $r+t\in\mathbb{Q}$. Then since $\mathbb{Q}$ is closed under taking multiplication and addition, $(t+r)+(-1)r$ is rational $\implies$ t is rational, contradiction. Hence, $r+t$ must be irrational.

(c) For $0\le k\le n$ we have
$$\binom{n}{k}=\binom{n}{n-k}.$$
True. This is the symmetry in the Pingala-Khayyam-YangHui-Pascal Triangle. Best proof is to notice that selecting a subset S of k elements from the set $\{1,2,\dots n\}$ is equivalent to selecting $n-k$ elements NOT to be in the set (i.e., selecting S^C). It can also be shown from the formula as in the text, Prop. 4.31.

(d) If $x\equiv a \pmod{m}$ and $x\equiv a \pmod{n}$, then $x\equiv a \pmod{mn}$.
False. $5\equiv 35 \pmod{6}$ and $5\equiv 35 \pmod{10}$, but $5\not\equiv 35 \pmod{60}$.
SALVAGE: True if $(m,n)=1$.

Proof. By hypothesis we have $m \mid x-a$ and $n \mid x-a$. Since $(m,n)=1$, this implies that $mn \mid x-a \implies$, which is what we want to show. ■

7. Make sure you know how to prove the following facts from the text.

(a) Every integer $n > 1$ can be written as a product of primes (not necessarily uniquely). [Via strong induction.]

(b) For $1 \leq r \leq n$

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$$

(c) (Euler-Fermat) If m is a positive integer and $(a, m) = 1$, then

$$a^{\varphi(m) \equiv 1 \pmod{m}}.$$

(d) There are numbers which are not rational.