Math373 **Quiz 12** **Wed. Apr 16, 2014**

Name: Solutions

Directions: Show all work. No credit for answers without work.

1. **[4 parts, 1 point each]** True/False. Mark each of the following statements as "True" or "False". To avoid ambiguity, write the entire word.

   (a) No primes have Miller–Rabin witnesses, but some primes have Fermat witnesses. FALSE

   (b) If a is a Fermat witness for n, then a is also a Miller–Rabin witness for n. TRUE

   (c) If n is composite, then at least 50% of $\mathbb{Z}_n^*$ are Fermat witnesses. FALSE – Carmichael #'s

   (d) If n is prime, then at least 75% of $\mathbb{Z}_n^*$ are Miller–Rabin witnesses. FALSE.

2. **[2 parts, 3 points each]** Let $n = 34241$. For the given values of a, determine whether a is a Miller–Rabin witness for the compositeness of n.

   (a) $a = 4872$

$n-1 = 34240 = 2^6 \cdot 535.$

i	0	1	2	3	4	5
$a^{2^i \cdot v}$	30242	1454	25415	1	1	1

$a^2 = 7371$

$a^4 = 25415$

$a^8 = 1.$

$a^{535} = (a^8)^{66} \cdot a^7$

$= 1 \cdot a^4 \cdot a^2 \cdot a$

$= 1454 \cdot 4872$

$= 30242$

Since $a^v \not\equiv 1$ and none of these is -1, a is a ~~Fermat~~ witness

MR

   (b) $a = 24993$

i	0	1	2	3	4	5
$a^{2^i v}$	16828	8514	34240 $\equiv -1$	1	1	1

$a^2 \equiv 25727$

$a^4 \equiv 34240$

$a^8 \equiv 1$

$a^{535} \equiv \cancel{(a^8)}^{66} \cdot a^7$

$\equiv a^4 \cdot a^2 \cdot a$

$\equiv 34240 \cdot 25727 \cdot 24993$

$\equiv -17413 \equiv 16828$

Since one of these powers of a is -1,

a is not a ~~Fermat~~ witness.

MR