REU PROBLEMS LIST AS OF 6/20/05

Let $n \geq 1$ be an odd integer. If a is an integer which satisfies the equivalence

$$a^{n-1} \equiv 1 \mod n$$

we say that n is a **pseudoprime to base** a . A composite n which is a pseudoprime to all bases $1 \leq a \leq n, (a, n) = 1$ is called a **Carmichael number**. The first few Carmichael numbers are $561, 1105, 1729, \ldots$

Problem 1. *Given n, is there a fast way to determine whether or not n is a Carmichael number?*

Let r and b be the unique positive integers for which $n - 1 = 2^r b$ and $2 \not| b$. We call n is a **strong pseudoprime to base a** if $\gcd(a, n) = 1$ and either

$$\begin{array}{lll} i) & a^b \equiv 1 \mod n, & \text{or} \\ ii) & a^{2^j b} \equiv -1 \mod n & \text{for some } 0 \leq j \leq r-1. \end{array}$$

It is a theorem that if n is composite then it can be a strong pseudoprime to base a for at most $1/4$ of the numbers $1 \leq a \leq n$ with $\gcd(a, n) = 1$. For composite n let witness(n) denote the smallest integer $a \geq 2$ with $\gcd(a, n) = 1$ and for which n is not a strong pseudoprime to base a.

Problem 2. *Find constants c_1 and $c_2 \in \mathbb{R}$ such that for all composite n,*

$$\text{witness}(n) \leq c_1 (\log n)^{c_2}.$$

Given n odd and composite define subsets S and G of $(\mathbb{Z}/n)^*$ by

$$\begin{aligned} S &= \{a \in (\mathbb{Z}/n)^* : n \text{ is a strong pseudoprime to base } a\} \quad \text{and} \\ G &= \left\{a \in (\mathbb{Z}/n)^* : a^{(n-1)/2} = \left(\frac{a}{n}\right)\right\}, \end{aligned}$$

where $(\frac{\cdot}{\cdot})$ denotes the Jacobi-Kronecker symbol. It is easy to show using the properties of this symbol that G is a subgroup of $(\mathbb{Z}/n)^*$. Write $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, and for each $1 \leq i \leq k$ let r_i and b_i be the unique positive integers for which $p_i - 1 = 2^{r_i} b_i$ and $2 \not| b_i$.

Problem 3. *Prove that S is not a subgroup of $(\mathbb{Z}/n)^*$ if and only if $k > 1$ and $p_i \equiv 1 \mod 4$ for all $1 \leq i \leq k$.*

(Solved by Zach Jones and Kichul Kim, see Kim's writeup).

Problem 4. *If S is a subgroup of $(\mathbb{Z}/n)^*$ then* witness(n) *must be prime. Is* witness(n) *always prime?*

The answer is known to be no. There are examples of n's for which witness(n) is any integer at most 12.

Problem 5. *Does every integer bigger than 1 occurs as* witness(n) *for some n?*

UT Austin: Summer 2005.

Problem 6. *Is it always true that*

$$|S| \leq \frac{\varphi(n)}{2^k}?$$

Can you classify the numbers for which this inequality fails to hold?

(Jamie Sloat found that there are counterexamples, the smallest of which is 8911. They all seem to be Carmichael numbers with $r_i = r$ for all i. Can you prove this?)

Problem 7. *Quantify the statement that if r is large and the r_i's are small, $|S|$ and $|G|$ should also be small.*

Problem 8. *There is a formula for $|G|$ in terms of n, r, k, and the p_i's, α_i's, and r_i's. Find a similar formula for $|S|$. Use it to show that, if S is not a subgroup of G, then $|S|$ does not divide $|G|$.*

(The formula for $|S|$ is in Kim's writeup, the second part of the problem is not yet done)

If $1, 2, \ldots, m$ are elements of G (or S, if S is a group), then any product formed with numbers from $1, 2, \ldots, m$ is also in G, thus forcing G to be large. This can be used to attack problem 2.

For $n \geq 0$ the n**th Fermat number** is defined to be $F_n = 2^{2^n} + 1$. The Fermat numbers are prime for $0 \leq n \leq 4$ and are known to be composite for $5 \leq n \leq 32$. It is conjectured that F_n is composite for $n \geq 5$.

Problem 9. *Is F_{33} prime or composite?*

For P and $Q \in \mathbb{Z}$ the **Lucas sequence generated by P and Q** is defined by

$$\begin{aligned} U_0 &= 0, \\ U_1 &= 1, \quad \text{and} \\ U_{n+2} &= PU_{n+1} - QU_n \text{ for } n \geq 0. \end{aligned}$$

The following test, due to Baillie, Pomerance, Selfridge, and Wagstaff, seems to be a very strong indicator of primes: Choose an odd number $n \geq 7$ which is not a square and check that

$$\begin{aligned} &i) \quad n \text{ is a strong pseudoprime to base 2, } \quad \text{and} \\ &ii) \quad U_{n+1} \equiv 0 \mod n, \end{aligned}$$

where $\{U_n\}$ is the Lucas sequence generated by $P = 1$ and $Q = (1 - D)/4$, with D being the first term in the sequence $5, -7, 9, -11, 13, \ldots$ with $\left(\frac{D}{n}\right) = -1$. It has been checked that this test correctly separates primes from composites for all $n \leq 10^{13}$. Furthermore, no composite number is known to pass this test.

Problem 10 (\$620 prize)**.** *Find a composite n which passes the BPSW test.*

Problem 11. *For a prime $p > 5$, the number $n = (4^p + 1)/5$ is always a strong pseudoprime to base 2 and composite. Does it ever pass the BPSW test?*

(It has been checked that these n's never pass the BPSW test for $p < 15000$, so the question is now better approached as a theoretical one).

Let n be an odd integer which is not a square and choose $D \in \mathbb{Z}$ so that $\left(\frac{D}{n}\right) = -1$. Define $H \subseteq \left((\mathbb{Z}/n)[\sqrt{D}]\right)^*$ by

$$H = \{x = a + b\sqrt{D} : x^n = a - b\sqrt{D}\}.$$

It is an exercise to show that H is a subgroup of $\left((\mathbb{Z}/n)[\sqrt{D}]\right)^*$.

Problem 12. *Is it true that* $H = \left((\mathbb{Z}/n)[\sqrt{D}]\right)^*$ *if and only if* n *is prime?*

(Kim showed that in this case n is either prime or a Carmichael number with $(p+1)|(n+1)$ for all $p|n$. There is no example of such Carmichael numbers and they will give composites passing the BPSW test)

Problem 13. *Find a formula for* $|H|$.

Problem 14. *Is it true that* $|H|$ *is small if* n *is composite?*

We can also consider $H' = \{x = a + b\sqrt{D} : x^n = a + bD^{(n-1)/2}\sqrt{D}\}$. and ask the same last three questions for H' instead of H, provided that H' is a group.

Problem 15. *When is* H' *a group?*

Let n be an r-AKS-pseudoprime if

$$(x+1)^n \equiv x^n + 1 \mod (n, x^r - 1).$$

Problem 16. *Find a composite* n *such that* r *doesn't divide* n *and* $n^2 - 1$ *and such that* n *is an* r*-AKS-pseudoprime. It seems that with* $r = 5$ *this is the same as finding a composite passing the BPSW test. A harder problem would be to a find such an* n *for each* r.

Problem 17. *Why is it easy to find (with the computer) composite* n *which are* r*-AKS-pseudoprimes with* $r|(n^2 - 1)$*?*

Problem 18. *Prove that if* $r > n/2$ *and* n *is an* r*-AKS-pseudoprime, then* n *is prime. Try to improve the inequality.*

Problem 19. *Show that if* n *is an* r*-AKS-pseudoprime, with* r *prime, then* n *passes a Lucas pseudoprime test with* $D = (-1)^{(r-1)/2}r$.

Let $R = \mathbb{Z}/n[x]/(h(x))$ for some polynomial $h(x)$, such that $h(x)|h(x^n)$ (For instance $h(x) = x^r - 1$ or $(x^r - 1)/(x - 1)$). Let

$$H = \{f(x) \in R^* \mid f(x)^n \equiv f(x^n) \mod h(x)\}.$$

Problem 20. *Find conditions on* $h(x)$ *under which* $H = R^*$ *if and only if* n *is prime.*

Problem 21. *Can you find formulas for* $|H|$ *similar to the quadratic case?*

Problem 22. *Show that if* n *is a prime power and*

$$(x+b)^n \equiv x^n + b \mod (n, x^r - 1).$$

for many b*'s then* n *is prime. That is, show that the first step of the AKS algorithm is unnecessary.*

Let R be as above and G the subgroup of R^* generated by $\{x+b|b \in B\}$ for some set $B \subset \mathbb{Z}/n$. The argument in the AKS proof shows that $|G| > 2^{|B|}$ if $\deg h > |B|$. The constant 2 has been improved and now stands at around 5.82.

Problem 23. *Is it true that* $|G| > c^{|B|\log|B|}$ *for some* $c > 1$ *under reasonable circumstances?*