HOMEWORK ASSIGNMENT #5 SOLUTIONS

This assignment has certain problems which require a fair amount of numerical calculation. Each problem has slightly different guidelines for the amount of calculation you should show on your work, so please check them carefully.

(1) Using the fast exponentiation algorithm for numbers mod n, compute $5^{87} \mod 307$ (that is, find the remainder when you divide 5^{87} by 307.) You can use a calculator to square numbers mod 307, and multiply individual numbers mod 307, but you should do the calculation of the binary expansion of the exponent by hand, list the appropriate table of powers of 5, and indicate why you are multiplying the correct powers together.

Solution. First we compute the binary expansion of $87 : 87 = 64+16+4+2+1 = 2^6+2^4+2^2+2^1+2^0$. Next we compute successive squares of $5 \mod 307$ until we reach 5^{64}, using a calculator:

$$5^2 \equiv 25 \mod 307, 5^4 \equiv 11 \mod 307, 5^8 \equiv 121 \mod 307,$$
$$5^{16} \equiv 212 \mod 307, 5^{32} \equiv 122 \mod 307, 5^{64} \equiv 148 \mod 307.$$

We now multiply together the appropriate powers of 5:

$$5^{87} \equiv 5^{64} \cdot 5^{16} \cdot 5^4 \cdot 5^2 \cdot 5^1 \equiv 148 \cdot 212 \cdot 11 \cdot 25 \cdot 5 \equiv 211 \mod 307.\square$$

(2) Show that 671 is a Fermat psuedoprime to the base 3. Same computational rules as the previous question.

Solution. This amounts to showing that 671 is composite and that $3^{670} \equiv 1 \mod 671$. The former is clear since $11 \mid 671$. For the latter, we calculate $3^{670} \mod 671$ using fast exponentiation. The binary expansion of 670 is $670 = 512 + 128 + 16 + 8 + 4 + 2$. We compute the relevant powers of $3 \mod 671$:

$$3^2 \equiv 9 \mod 671, 3^4 \equiv 81 \mod 671, 3^8 \equiv 522 \mod 671$$
$$3^{16} \equiv 58 \mod 671, 3^{128} \equiv 522 \mod 671, 3^{512} \equiv 9 \mod 671.$$

Therefore

$$3^{670} \equiv 9 \cdot 522 \cdot 58 \cdot 522 \cdot 81 \cdot 9 \equiv 1 \mod 671,$$

as desired.

(3) Show that $1105 = 5 \cdot 13 \cdot 17$ is a Carmichael number. You should only use a calculator to check whether a number is a divisor of another number.

Solution. We want to show that $a^{1105} \equiv a \mod 1105$ for all a. This is equivalent to showing that $a^{1105} \equiv a \mod 5, 13, 17$ for all a. For instance, to show that $a^{1105} \equiv a \mod 5$, this is automatically true if $5 \mid a$, and if $5 \nmid a$, then $a^4 \equiv 1 \mod 5$, and since 1105 divided by 4 has a remainder of 1, this shows that $a^{1105} \equiv a \mod 5$. Similarly, we see that 1105 divided by $13-1=12$ has a remainder of 1, and 1105 divided by $17-1=16$ also has a remainder of 1, so 1105 is Carmichael, as desired. $\square$

(4) Show that 2047 is a strong psuedoprime to the base 2. For this problem you should not use a calculator, at all. (There is probably a clever way to solve this problem. How are 2047 and 2 related?)

Solution. First, notice that $2047 - 1 = 2046 = 2 \cdot 1023$. Therefore, to show that 2047 is a strong psuedoprime to the base 2, we want to show that 2047 is composite, and that $2^{1023} \equiv 1 \mod 2047$, or that $2^{1023} \equiv -1 \mod 2047$. First, one sees that $2047 = 23 \cdot 89$, so 2047 is composite.

Next, notice that $2047 = 2^{11} - 1$. Therefore, $2^{11} \equiv 1 \mod 2047$. On the other hand, $11 \mid 1023$, so $2^{1023} \equiv 1 \mod 2047$. Therefore 2047 is a strong pseudoprime to base 2. $\square$

(5) Show that 91 is a psuedoprime to the base 3, but not a strong psuedoprime to base 3. Same computational rules as the first two questions.

Solution. Clearly 91 is composite, since $91 = 7 \cdot 13$. Also, $91 - 1 = 90 = 2 \cdot 45$, so we want to show that $3^{90} \equiv 1 \mod 91$, but that $3^{45} \not\equiv \pm 1 \mod 91$. We compute $3^{45} \mod 91$ using successive squaring. The binary expansion of 45 is $45 = 32 + 8 + 4 + 1$, and

$$3^4 \equiv 81 \mod 91, 3^8 \equiv 9 \mod 91, 3^{32} \equiv 9 \mod 91,$$

so $3^{45} \equiv 9 \cdot 9 \cdot 81 \cdot 3 \equiv 27 \mod 91$, which evidently is not $\pm 1 \mod 91$. On the other hand, $3^{90} \equiv 27^2 \equiv 1 \mod 91$. So 91 is a psuedoprime to base 3, but not a strong psuedoprime to base 3. $\square$

(6) Let $a \geq 2$ be a positive integer, and let p be an odd prime not dividing $a^2 - 1$. Show that $\dfrac{a^{2p} - 1}{a^2 - 1}$ is a Fermat psuedoprime to the base a. (Notice, in particular, that this implies that there are infinitely many Fermat psuedoprimes to base a.)

Solution. First, we check that $\dfrac{a^{2p} - 1}{a^2 - 1}$ is composite. Indeed, notice that

$$\frac{a^{2p} - 1}{a^2 - 1} = \frac{a^p - 1}{a - 1} \cdot \frac{a^p + 1}{a + 1}.$$

The first fraction is the integer $1 + a + a^2 + \ldots + a^{p-1}$, and is obviously greater than 1, since $p \geq 3, a \geq 2$. The second fraction is also an integer, equal to $1 - a + a^2 - \ldots + a^{p-1}$. (This is one place where we use p being odd.) This integer is also greater than 1, since $a^p \neq a + 1$. Therefore this gives a genuine factorization of $\dfrac{a^{2p} - 1}{a^2 - 1}$ into proper divisors.

Let $n = \dfrac{a^{2p} - 1}{a^2 - 1}$. We want to show that $a^{n-1} \equiv 1 \mod n$. First, notice that $n - 1 = \dfrac{a^{2p} - a^2}{a^2 - 1}$. We know that $a^p \equiv a \mod p$, regardless of the value of a, so squaring both sides we get $a^{2p} \equiv a^2 \mod p$, which tells us that $p \mid (a^{2p} - a^2)$. On the other hand, by assumption $p \nmid a^2 - 1$. Therefore, $p \mid (n - 1)$. Also, notice that $n = 1 + a^2 + a^4 + \ldots + a^{2p-2}$. This is a sum of 1 with $p - 1$ terms of the form $a^{2i}, 1 \leq i \leq p - 1$. Regardless of whether a is even or odd, because $p - 1$ is even, the sum of the a^{2i} terms is even, so $n-1$ is even. This means that $2 \mid (n-1)$. Since $2, p$ are coprime, this implies that $2p \mid n-1$ as well.

Notice that $a^{2p} \equiv 1 \mod (a^{2p}-1)$. This means that $a^{n-1} \equiv 1 \mod (a^{2p}-1)$. But this modulus is $a^{2p}-1$, which is a multiple of n, so $a^{n-1} \equiv 1 \mod n$ is true as well, as desired. □

(7) Find all solutions to $x^2 + 3x + 7 \equiv 0 \mod 5^3$. You should not use a calculator for this problem.

Solution. First, we find solutions to $x^2 + 3x + 7 \equiv 0 \mod 5$. Inspection yields the solutions $x \equiv 3, 4 \mod 5$. (Indeed, notice that $x^2 + 3x + 7 \equiv x^2 + 3x + 2 \equiv (x+1)(x+2) \mod 5$.)

We use Hensel's Lemma to attempt to lift these to solutions mod 5^3. First, start with $x_1 = 3$. Letting $f(x) = x^2 + 3x + 7$, we get $f'(x) = 2x + 3$, so $f'(x_1) = 9$, and $5 \nmid 9$, so Hensel's Lemma tells us there is a unique left of $3 \mod 5$ to a solution mod 5^2. To find this solution, we first compute $f(x_1) = f(3) = 25 = 5 \cdot 5$. We want to solve the linear congruence $5 + 9k_1 \equiv 0 \mod 5$, which obviously has unique solution $k_1 \equiv 0 \mod 5$. This means that $x_1 = 3$ lifts to a solution $x_2 = 3 + k_1 \cdot 5 = 3$ mod 25.

We use Hensel's Lemma again; this time $f(x_2) = f(3) = 25 = 1 \cdot 5^2$. Therefore we want to solve the linear equation $1 + 9k_2 \mod 5$; this has unique solution $k_2 \equiv 1$ mod 5, so $x_2 = 3$ lifts to the solution $x_3 = x_2 + k_2 5^2 = 3 + 25 \equiv 28 \mod 125$.

We do the same thing with $x_1 = 4$. This time, $f'(x_1) = f'(4) = 11$, and $5 \nmid 11$, so this solution lifts uniquely to modulus 5^2. We also have $f(x_{1)} = f(4) = 35 = 7 \cdot 5$, so to find the lift solution, we want to solve the linear congruence $7 + 11k_1 \equiv 0 \mod 5$. This clearly has unique solution $k_1 \equiv 3 \mod 5$, so $x_1 = 4$ lifts to $4 + 3 \cdot 5 = 19$ mod 25.

Since $19 \equiv 4 \mod 5$, we still know that $5 \nmid f'(19)$, so $x_2 = 19$ lifts uniquely to a solution mod 5^3. Also, $f(x_2) = f(19) = 425 = 17 \cdot 25$. Therefore we want to solve the linear congruence $17 + k_2 \equiv 0 \mod 5$, which has unique solution $k_2 \equiv 3$ mod 5. This shows that $x_2 = 17$ lifts to a solution $19 + 3 \cdot 25 = 94 \mod 125$. □

(8) (a) Show that $x^2 \equiv 2 \mod 5^n$ has no solution, for any $n \geq 1$.
(b) Show that $x^2 \equiv 2 \mod 7^n$ has a solution, for any $n \geq 1$.

Solution.

(a) Notice that $x^2 \equiv 2 \mod 5$ has no solutions, since $x^2 \equiv 0, 1, 4 \mod 5$ if x is an integer. Therefore $x^2 \equiv 2 \mod 5^n$ cannot possibly have any solutions either.
(b) First, notice that $x^2 \equiv 2 \mod 7$ has a solution $x \equiv 3 \mod 7$. We claim we can repeatedly lift this, using Hensel's Lemma, to solutions mod 7^n. Indeed, suppose we have a solution x_i to $x^2 \equiv 2 \mod 7^i$, satisfying $x_i \equiv 3 \mod 7$. Since $f(x) = x^2 - 2$, $f'(x) = 2x$, so $7 \nmid f'(x_i)$. Hensel's Lemma says that x_i lifts uniquely to a solution $x_{i+1} \mod 7^{i+1}$, and since $x_{i+1} \equiv x_i \mod 7^i$, this means that $x_{i+1} \equiv x_i \equiv 3 \mod 7$. □