Math 3240 - Introduction to Number Theory — Due by email
Problem Set 2 — 2/22/20 at noon

Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.
[*God made the integers, all else is the work of man.*] Kronecker

- Required Reading: "Unique Factorization" and "Quadratic Integers".
- Optional: "Universal Divisibility Test" and "Analogies with Polynomials".

1. (Induction practice)

   a) (**10 pts**) If $a \equiv b \bmod 2^r$ where $r \geq 1$, prove by induction that $a^{2^k} \equiv b^{2^k} \bmod 2^{r+k}$ for all $k \geq 0$. (Note the base case is $k = 0$, not $k = 1$.) The upshot is that successive squaring "improves" 2-power congruences. (Hint: Write the congruence modulo 2^r as an equation in $\mathbf{Z}$ and use the formula for $(x+y)^2$ before reducing modulo 2^{r+1}.)[1]

   Then adapt the technique to state and prove a similar result for 3-power congruences: if $a \equiv b \bmod 3^r$ where $r \geq 1$, prove by induction that $a^{3^k} \equiv b^{3^k} \bmod 3^{r+k}$ for all $k \geq 0$.

   b) (**10 pts**) Write every positive integer from 1 to 10 as a sum and difference of different powers of 3. Examples are $23 = -1 - 3 + 3^3$, $30 = 3 + 3^3$, and $17 = -1 - 3^2 + 3^3$, but *not* $17 = -1 + 3^2 + 3^2$ because 3^2 appears twice. Then prove by induction that every $a \in \mathbf{Z}^+$ has such a representation: $a = c_0 + 3c_1 + 9c_2 + \cdots + 3^d c_d$ for some $d \geq 0$, where each c_i is 0, 1, or -1. (Hint: Modify the method of proving ordinary base expansions exist in $\mathbf{Z}^+$.)

2. (Exploration)

   a) (**7 pts**) You know 5^2 ends in a 5 and 6^2 ends in a 6. Some of you might have known that $25^2 = 6\mathbf{25}$ ends in 25. There's another 2-digit example: $76^2 = 5\mathbf{776}$ ends in 76. But why stop at two digits? Use Wolfram Alpha to find as many three-digit numbers x as you can such that "x^2 ends in x" and push the search for such numbers through at least 6 digits. Explain how you use Wolfram Alpha to carry out the search.

   b) (**6 pts**) A popular sequence in elementary mathematics is the Fibonacci sequence: $F_1 = 1$, $F_2 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n > 2$. The first 20 terms in the Fibonacci sequence are

   $$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765.$$

   For any $m > 1$ we can reduce the Fibonacci numbers modulo m. The first 20 terms of the Fibonacci sequence reduced modulo 3 are

   $$\mathbf{1, 1, 2, 0, 2, 2, 1, 0}, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, 2, 2.$$

   This is a periodic sequence, with period 8 (the periodic part is in bold). The table below indicates for all primes p below 150, other than 2 and 5, the period of $F_n \bmod p$.

p	3	7	11	13	17	19	23	29	31	37	41
period($F_n \bmod p$)	8	16	10	28	36	18	48	14	30	76	40
p	43	47	53	59	61	67	71	73	79	83	89
period($F_n \bmod p$)	88	32	108	58	60	136	70	148	78	168	44
p	97	101	103	107	109	113	127	131	137	139	149
period ($F_n \bmod p$)	196	50	208	72	108	76	256	130	276	46	148

[1] Don't use bad algebra like rewriting $a^{2^{k+1}}$ as $a^{2^k} a^2$, which is completely wrong.

What patterns do you notice in these periods? (Think about *divisibility* seriously and the patterns from the periodic parts of decimal expansions of $1/p$ on Exercise 2b on Set 1.)

c) (**7 pts**) For each prime $p = 2, 3, 5, 7, 11, 13, 17, 19$, use Exercise 2c on Set 1 to show explicitly that every number modulo p has the form $x^2 + y^2$. That is, for $0 \leq a \leq p-1$, find a solution to the congruence $x^2 + y^2 \equiv a \bmod p$. Actually, since the numbers 0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, and 18 are sums of two squares in $\mathbf{Z}$ (e.g., $2 = 1 + 1$ and $13 = 4 + 9$), they are automatically sums of two squares mod p so there is no point in tabulating results in those cases. Just prepare a list for $a = 3$, 6, 7, 11, 12, 14, and 15 by filling in the table below, where the first row lists the primes p and the first column lists the a's to be written as a sum of two squares mod p. (One of the squares might be 0.) A few entries are filled in already, *e.g.*, $6 \equiv 9 + 10 \bmod 13$ and 9 and 10 are squares mod 13. Replace the question marks with sums of two squares mod p.

p	5	7	11	13	17	19
3	$4+4$	?	?	$0+3$	?	?
6		?	?	$9+10$	?	?
7			?	?	?	?
11				?	$13+15$	?
12				?	?	?
14					?	?
15					?	?

3. (Simultaneous congruences)

a) (**10 pts**) Find all solutions to the simultaneous congruences $x \equiv 1 \bmod 7$ and $x \equiv 3 \bmod 10$ by using the systematic method discussed in class: write the first congruence in the form $x = 1 + 7y$ for unknown $y \in \mathbf{Z}$ and substitute this into the second congruence and solve for y. (The moduli are small, so you may find inverses by inspection rather than by Euclid.) Your final answer should be a single congruence condition on x.

b) (**10 pts**) Repeat the technique in part a to find all solutions to $x \equiv a \bmod 7$ and $x \equiv b \bmod 10$ where a and b are general integers. Your final answer will be a single congruence condition on x involving a and b and had better specialize to your answer in part a when $a = 1$ and $b = 3$.

4. (Base expansions)

Read the section on base expansions for integers and polynomials in Section 5 of the handout on the division algorithm.

a) (**10 pts**) Use successive division by the base to figure out the representation of 1881 in bases 6, 7, 9, 11, and 12. (If you need "digits" in bases 11 and 12 beyond the digit 9, use A for the digit 10 and B for the digit 11).

b) (**10 pts**) Use successive division by the base to figure out the representation of the polynomial $T^6 - T^4 + 5T + 3 \in \mathbf{Q}[T]$ in bases $T - 1$, $T^2 + 1$, $2T^2 + T$, T^3, and $T^3 - 2$. You can use a computer algebra system to compute the polynomial division, but write out the results of each calculation clearly and *proofread what you write.*

5. (Prime factorization in a new setting)

Fix an integer d that is not a perfect square. We define $\mathbf{Z}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbf{Z}\}$. For instance, some numbers in $\mathbf{Z}[\sqrt{2}]$ are $3 + \sqrt{2}$ and $9 - 8\sqrt{2}$, but *not* $\frac{2}{3} + \sqrt{2}$. Note $\mathbf{Z} \subset \mathbf{Z}[\sqrt{d}]$

since $x = x + 0\sqrt{d}$ for all integers x. The sum, difference, and product of two numbers in $\mathbf{Z}[\sqrt{d}]$ are again in $\mathbf{Z}[\sqrt{d}]$ since

$$(x_1 + y_1\sqrt{d}) \pm (x_2 + y_2\sqrt{d}) = (x_1 + x_2) \pm (y_1 + y_2)\sqrt{d}$$

and

$$(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = (x_1x_2 + dy_1y_2) + (x_1y_2 + x_2y_1)\sqrt{d}.$$

For any $\alpha = x + y\sqrt{d}$ in $\mathbf{Z}[\sqrt{d}]$, its *norm* is

$$\mathrm{N}(\alpha) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2.$$

The norm is in $\mathbf{Z}$. As examples, $\mathrm{N}(2 + \sqrt{-7}) = 11$ and $\mathrm{N}(4 + 5\sqrt{2}) = -34$, so norms can be negative (if $d > 0$). If $x \in \mathbf{Z}$ then $\mathrm{N}(x) = x^2$. In class it will be shown that $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$ for all α and β in $\mathbf{Z}[\sqrt{d}]$, no matter what d is.

a) (**10 pts**) In $\mathbf{Z}[i]$, where $d = -1$, we have $\mathrm{N}(x + yi) = x^2 + y^2$. Compute the norms of $2 + i$, $2 - 3i$, and $3 + 4i$. In $\mathbf{Z}[\sqrt{7}]$, compute the norms of $127 + 48\sqrt{7}$ and $37 + 14\sqrt{7}$.

b) (**10 pts**) Call $\alpha \in \mathbf{Z}[\sqrt{d}]$ *composite* if $|\,\mathrm{N}(\alpha)| > 1$ and there is a factorization $\alpha = \beta\gamma$ for some β and γ in $\mathbf{Z}[\sqrt{d}]$ such that $|\,\mathrm{N}(\beta)| < |\,\mathrm{N}(\alpha)|$ and $|\,\mathrm{N}(\gamma)| < |\,\mathrm{N}(\alpha)|$. Call $\alpha \in \mathbf{Z}[\sqrt{d}]$ *prime* if $|\,\mathrm{N}(\alpha)| > 1$ and α is not composite. For instance $3 + i$ is composite in $\mathbf{Z}[i]$ since $|\,\mathrm{N}(3 + i)| = 10$ and $3 + i = (1 + 2i)(1 - i)$, where the factors have norm 5 and 2. **Warning**: Saying α in $\mathbf{Z}[\sqrt{d}]$ is prime is not equivalent to saying $|\,\mathrm{N}(\alpha)|$ is a prime number. For instance, it can be shown that $1 + \sqrt{5}$ is prime in $\mathbf{Z}[\sqrt{5}]$ even though $|\,\mathrm{N}(1 + \sqrt{5})| = 4$.

Your task: in each $\mathbf{Z}[\sqrt{d}]$, use induction on the absolute value of the norm on $\mathbf{Z}[\sqrt{d}]$ to prove that every $\alpha \in \mathbf{Z}[\sqrt{d}]$ satisfying $|\,\mathrm{N}(\alpha)| > 1$ can be written as a product of primes in $\mathbf{Z}[\sqrt{d}]$. Do *not* try to prove uniqueness of the prime factorization; just prove prime factorization in $\mathbf{Z}[\sqrt{d}]$ exists. In your argument, the choice of d should remain general, *e.g.*, the base case can't be for only one value of d like $d = -1$. (Hint: Extend the proof from class that every positive integer > 1 is a product of prime numbers.)