If 90% of the ideas you generate aren't absolutely worthless, then you're not generating enough ideas. —Michael Artin

1. Carmichael numbers:
   (a) Prove that 1105 is a Carmichael number by showing that for each prime factor $p \mid 1105$, and for every a s.t. $(a, 1105) = 1$, $a^{1104} \equiv 1 \pmod{p}$, whence the same holds mod 1105.
   (b) Let $n = p_1 p_2 \cdots p_r$ be a product of *distinct* primes such that $p_i - 1 \mid n - 1$ for every $i = 1, 2, \ldots r$. Show that n is a Carmichael number.
   (c) Give three examples of numbers > 2000 which satisfy the hypotheses above and hence are Carmichael numbers.

2. Prove or Disprove and Salvage if Possible. Try to prove your salvages.
   (a) No Carmichael number is divisible by a perfect square > 1.
   (b) For $p \in \mathbf{Z}^+$, $(p-1)! \equiv -1 \pmod{p} \iff p$ is prime.
   (c) If $\varphi(n) \mid (n-1)$, then n is a square-free integer.
   (d) For all $a, m, n \in \mathbf{Z}^+$, $(a^n - 1, a^m - 1) = (a^{(n,m)} - 1)$

3. Numerical Problems
   (a) Find the smallest Fermat witness for 2701.
   (b) Let $m = 512,461$. Use Wolfram Alpha to check whether any values $2 \leq a \leq 11$ are Fermat witnesses for m. What do you find? Does this tell you anything for certain about whether m is prime or not?
   (c) Describe an infinite set of integers which all satisfy $\varphi(n) \mid n$.
   (d) Find the last two digits of the decimal representation of 3^{F_5}, where $F_5 = 2^{2^5} + 1$ is the fifth Fermat number.

4. Exploration of squares in $\mathbf{Z}/p$
   (a) Look at **both** files "Squares Modulo Primes" and "Primes and Congruence Conditions", which both concern primes up to 200, **together**. Writing $\Box$ for an unknown square, conjecture from the files a set of congruence conditions on all primes p which characterize those for which $-1 \equiv \Box \bmod p$, with finitely many possible exceptions. Your characterization should account for all $p < 200$ for which $-1 \equiv \Box \bmod p$ *and* not include any $p < 200$ for which $-1 \not\equiv \Box \bmod p$.

      Then do the same for each of the conditions $2 \equiv \Box \bmod p$, $-2 \equiv \Box \bmod p$, $3 \equiv \Box \bmod p$, $-3 \equiv \Box \bmod p$, $5 \equiv \Box \bmod p$, and $-5 \equiv \Box \bmod p$. The last case, with -5, will be harder than the rest!

(b) For $m = 11, 14, 18$, and 22, find a generator for the units mod m and explicitly show that the powers of your generator run through all the units modulo m.

In the file "Moduli with a Generator for the Units" is a table of all moduli below 302 where the units have a generator. Propose a general characterization of the $m \geq 2$ for which the units modulo m have a generator. Your characterization should not only include all integers $m \leq 302$ which appear in the table but also *exclude* all positive integers up to 302 which are not in the table. (Hint: Consider first odd m, then even m.)

5. **Arithmetic in $\mathbf{Z}[\sqrt{\mathbf{d}}]$:** For any non-square $d \in \mathbf{Z}$, let

$$\mathbf{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbf{Z}\}.$$

For example,

$$\mathbf{Z}[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \mathbf{Z}\} = \{0, 6, \sqrt{5}, 7 + 4\sqrt{5}, -9 + 11\sqrt{5}, \dots\}.$$

The elements of $\mathbf{Z}[\sqrt{d}]$ are closed under addition, subtraction, and multiplication. (The case $d = -1$ is the Gaussian integers.) For $\alpha = a + b\sqrt{d}$ in $\mathbf{Z}[\sqrt{d}]$, set the *norm* of α to be $\mathrm{N}(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \in \mathbf{Z}$. For example, the norm of $7 + 4\sqrt{5}$ is $7^2 - 5 \cdot 4^2 = -31$, so norms can be negative.

We say $\alpha \in \mathbf{Z}[\sqrt{d}]$ is a *unit* when it has a multiplicative inverse: $\alpha\beta = 1$ for some $\beta \in \mathbf{Z}[\sqrt{d}]$.

(a) Show $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$ for all α and β in $\mathbf{Z}[\sqrt{d}]$.

(b) Prove $\alpha \in \mathbf{Z}[\sqrt{d}]$ is a unit if and only if $\mathrm{N}(\alpha) = \pm 1$.

(c) If $uv = 1$ then $u^n v^n = 1$ for any integer n, so any integral power of a unit is a unit. Show $1 + \sqrt{2}$ is a unit in $\mathbf{Z}[\sqrt{2}]$ and then compute the first 8 powers of $1 + \sqrt{2}$ in the form $a + b\sqrt{2}$. Where have you seen the coefficients of some of these powers earlier in the course?

(d) Two obvious units in $\mathbf{Z}[\sqrt{d}]$ are ± 1. For $d = 3, 5, 6, 7, 8, 10, 11$, and 12, find a unit in $\mathbf{Z}[\sqrt{d}]$ other than ± 1 and list for each unit what its inverse is. (Be sure your inverses are correct!) What can you say about units in $\mathbf{Z}[\sqrt{d}]$ if $d < 0$ and $d \neq -1$?

(e) A *unit multiple* of $\alpha \in \mathbf{Z}[\sqrt{d}]$ is a product αu, where u is a unit in $\mathbf{Z}[\sqrt{d}]$. (For instance, one unit multiple of $5 + \sqrt{2}$ is $(5 + \sqrt{2})(1 + \sqrt{2}) = 7 + 6\sqrt{2}$.) For any unit u in $\mathbf{Z}[\sqrt{d}]$, show u and αu are divisors of α. (Units and unit multiples of α are considered the trivial divisors of α, just like ± 1 and $\pm n$ are trivial divisors of an integer n.)

(f) When $\alpha \in \mathbf{Z}[\sqrt{d}]$ is not a unit (*i.e.*, $|\,\mathrm{N}(\alpha)| > 1$ by part b), call α *prime* if its only divisors in $\mathbf{Z}[\sqrt{d}]$ are units and unit multiples of α, as in part e. If $\mathrm{N}(\alpha) = \pm p$ for a prime number p, show α is prime in $\mathbf{Z}[\sqrt{d}]$. Then use this to give examples of four primes in $\mathbf{Z}[\sqrt{3}]$ with different norms.

(g) Call a nonzero $\alpha \in \mathbf{Z}[\sqrt{d}]$ *composite* if it is not a unit and not a prime. Show α is composite if and only if it has a factorization $\alpha = \beta\gamma$ where $|\,\mathrm{N}(\beta)| < |\,\mathrm{N}(\alpha)|$ and $|\,\mathrm{N}(\gamma)| < |\,\mathrm{N}(\alpha)|$. Then use induction on the absolute value of the norm to prove every $\alpha \in \mathbf{Z}[\sqrt{d}]$ with $|\,\mathrm{N}(\alpha)| > 1$ is a product of primes in $\mathbf{Z}[\sqrt{d}]$.