SOLUTIONS to Sample Exam

1. (a) We assume $ab \neq 0$. (If $a = b = 0$ then $\gcd(a,b)$ is undefined; if exactly one of a, b is zero then $\gcd(a,b) = \max\{|a|,|b|\}$.) Repeatedly divide:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\cdots \\ r_{n-1} &= q_{n+1} r_n + r_{n+1} \\ r_n &= q_{n+2} r_{n+1} + 0 \end{aligned}$$

where $b > r_1 > r_2 > \cdots > r_{n+1} > 0$. Then $\gcd(a,b) = r_{n+1}$ is the last nonzero remainder. This algorithm works quite well, even for reasonably large integers.

(b) The *extended form* of Euclid's Algorithm finds integers k, ℓ such that $ka + \ell b = \gcd(a,b)$. To see this, using the notation of (a) we start with

$$r_{n+1} = (*)r_n + (*)r_{n-1}$$

where the coefficients $(*)$ are integers. Eliminate $r_n, r_{n-1}, \ldots, r_1$ in that order, in each case using the previous equation. This yields

$$\begin{aligned} \gcd(a,b) = r_{n+1} &= (*)r_n + (*)r_{n-1} \\ &= (*)r_{n-1} + (*)r_{n-2} \\ &\cdots \\ &= (*)r_2 + (*)r_1 \\ &= (*)r_1 + (*)b \\ &= (*)b + (*)a. \end{aligned}$$

Thus, given $a, m \in \mathbb{Z}$ with $\gcd(a,m) = 1$, we are able to find integers k, ℓ satisfying $ka + \ell m = 1$. It follows that k is the inverse of $a \mod m$. This algorithm works quite well, even for moderately large integers a, m.

(c) As explained in (b), we can find $k \in \mathbb{Z}$ such that $ka \equiv 1 \mod m$; then $x \equiv kax \equiv kb \mod m$. This also works quite well for reasonably large integers.

2. From $\gamma = 2 + \frac{1}{1+\frac{1}{\gamma}}$ we obtain $\gamma^2 - 2\gamma - 2 = 0$, so $\gamma = \frac{2\pm\sqrt{12}}{2} = 1 \pm \sqrt{3}$. Since $\gamma > 0$, we have $\gamma = 1 + \sqrt{3}$.

3. (a) $\phi(3000) = \phi(2^3{\cdot}3{\cdot}5^2) = 2^2{\cdot}2{\cdot}(5^3{-}5^2) = 800$.

(b) $\sigma(3000) = \sigma(2^3{\cdot}3{\cdot}5^2) = (2^4{-}1)(3+1)\left(\frac{5^4-1}{5-1}\right) = 9360$.

(c) By Fermat's Little Theorem, $2^{98} = 2^{96}{\cdot}2^2 \equiv 2^2 \equiv 4 \mod 97$.

(d) $\left(\frac{82}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{41}{97}\right)\left(\frac{15}{41}\right) = \left(\frac{3}{41}\right)\left(\frac{5}{41}\right) = \left(\frac{41}{3}\right)\left(\frac{41}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{1}{5}\right) = (-1)(1) = -1$.

(e) The discriminant is $4^2 - 4{\cdot}73 = -276 \equiv 105 \mod 127$. Now $\left(\frac{105}{127}\right) = \left(\frac{3}{127}\right)\left(\frac{5}{127}\right)\left(\frac{7}{127}\right)$ $= (-1)\left(\frac{127}{3}\right)\left(\frac{127}{5}\right)(-1)\left(\frac{127}{7}\right) = \left(\frac{1}{3}\right)\left(\frac{2}{5}\right)\left(\frac{1}{7}\right) = (1)(-1)(1) = -1$. Since the discriminant is a nonsquare, there are *no* solutions to the given congruence.

4. The only primes $p < 30$ of the form $a^2 + 3b^2$ are

$$\begin{aligned} 3 &= 0^2 + 3{\cdot}1^2, \\ 7 &= 2^2 + 3{\cdot}1^2, \\ 13 &= 1^2 + 3{\cdot}2^2, \\ 19 &= 4^2 + 3{\cdot}1^2. \end{aligned}$$

(b) *Conjecture:* A prime p is expressile in the form $a^2 + 3b^2$ iff $p \equiv 0$ or $1 \mod 3$.

(c) For $a \in \mathbb{Z}$, we have $a^2 \equiv 0$ or $1 \mod 3$, so $a^2 + 3b^2 \equiv 0$ or $1 \mod 3$. Thus no prime $p \equiv 2 \mod 3$ is expressible in the form $a^2 + 3b^2$.

5. (a) A *Mersenne prime* is a prime of the form $2^p - 1$ where p is prime. The smallest Mersenne primes are $2^2{-}1 = 3$, $2^3{-}1 = 7$, $2^5{-}1 = 31$, $2^7{-}1 = 127$.

(b) A *perfect number* is a positive integer which equals the sum of its positive proper divisors. The smallest examples are $2(2^2{-}1) = 6$ and $2^2(2^3{-}1) = 28$.

(c) A *primitive Pythagorean triple* is a triple (a, b, c) of positive integers, any two of which are relatively prime, such that $a^2 + b^2 = c^2$. Two of the smallest examples are $(3, 4, 5)$ and $(5, 12, 13)$.

6. By inspection (or by continued fractions), one solution is $10^2 - 11{\cdot}3^2 = 1$. Thus $N(10 + 3\sqrt{11}) = 1$ where $N : \mathbb{Q}[\sqrt{11}] \to \mathbb{Q}$ is the norm map. We have

$$(10 + 3\sqrt{11})^2 = 199 + 60\sqrt{11}; \quad (10 + 3\sqrt{11})^3 = 3970 + 1197\sqrt{11}\,.$$

The smallest solution with $y > 100$ is $(x, y) = (3970, 1197)$.

7. (a) We know from the general theory that there exists a nontrivial integer solution of Pell's equation $a^2 - 21b^2 = 1$. (The smallest such solution is $(a, b) = (55, 12)$, by the way, although the question does not require an explicit solution.) For each $k \in \mathbb{Z}$, the element $a_k + b_k\sqrt{21} = (a + b\sqrt{21})^k \in Z[\sqrt{21}]$ gives infinitely many solutions of Pell's equation. So we have infinitely many solutions $(2a_k, 2b_k)$ of $x^2 - 21y^2 = 4$.

(b) Since every integer square is congruent to one of $0, 1, 4, 7 \mod 9$, the expression $x^2 - 21y^2$ reduces to one of $0, 1, 4, 6, 7 \mod 9$, never 8; so the equation $x^2 - 21y^2 = -1$ has no integer solutions.

8. (a) $3.14 = 3 + \frac{7}{50} = 3 + \frac{1}{50/7} = 3 + \frac{1}{7+\frac{1}{7}} = [3,7,7]$. The continued fraction expression $[3,7,6,1]$ is also correct.

   (b) $1+\sqrt{3} = [\overline{2,1}]$ as in #2. (Whoops, I didn't intend to repeat this value. The continued fraction expansion is also easy to find from the decimal expansion.)

9. There are exactly two solutions, which are the roots of $x^4-4 = (x^2-2)(x^2+2)$ in the field $\mathbb{F}_p$ of order p. Note that $\left(\frac{-1}{p}\right) = -1$.

   - If $p \equiv 3 \mod 8$, then $\left(\frac{2}{p}\right) = -1$ and $\left(\frac{2}{p}\right) = 1$. In this case, x^2-2 has no roots, and x^2+2 has two roots in $\mathbb{F}_p$.
   - Otherwise, $p \equiv 7 \mod 8$, and it is the other way around. Here $\left(\frac{2}{p}\right) = 1$ and $\left(\frac{2}{p}\right) = -1$. In this case, x^2-2 has two roots, and x^2+2 has no roots in $\mathbb{F}_p$.

10. (a) F (b) F (c) F (d) T (e) T (f) F (g) F (h) F (i) F (j) T

Comments in #10:

(a) $\pi(n) \sim \frac{n}{\ln n}$ so $\frac{\pi(n)}{\ln n} \sim \frac{n}{(\ln n)^2} \to \infty$ as $n \to \infty$.

(b) It is an open problem whether or not there are infinitely many primes of the form n^2+1.

(c) As discussed in class, finding square roots mod m is as difficult as factoring m. This is prohibitively difficult if m has hundreds of digits (unless m is already prime).

(d) There are infinitely many rational points on the unit circle, corresponding to points of the form $(\pm\frac{a}{c}, \pm\frac{b}{c})$ where (a,b,c) ranges over the infinite set of primitive Pythagorean triples. (Together with the trivial points $(\pm1,0)$, $(0,\pm1)$, this gives *all* the rational points on the unit circle.)

(e) One explanation uses the fact that n is expressible as a sum of two squares, iff there is no prime $p \equiv 3 \mod 4$ for which the highest power of p dividing n has *odd* exponent. Note that n satisfies this condition iff $13n$ does.

(f) This sounds like a converse of the Riemann Hypothesis, and it is certainly false. (Any complex analytic function vanishing on the line $Re(z) = \frac{1}{2}$ is forced to be trivial (zero everywhere). The Riemann zeta function is zero at just a countably infinite set of points.

(g) A counterexample is given by $n = N! + 2$ where $N = 10^{10} + 2$. Note that, as explained in class, the sequence of prime numbers has arbitrarily large gaps.

(h) If $a \equiv b \mod 6$ then $3^a \equiv 3^b \mod 7$, by Fermat's Little Theorem. (For a counterexample to the statemement given, try $a = 7$ and $b = 0$.)

(i) 'RSA' stands for Rivest, Shamir, Adleman—the three co-inventors of a celebrated public key encryption scheme, not an algorithm for factoring. Don't confuse this with the rho method for factorization (which is not actually considered a modern method).

(j) This follows by Dirichlet's Theorem.