Math 116
Final Problem Set Solutions

Six problems were graded, in two groups:
A: Problems 4.4, 11.4 and cumulative problem 2;
B: Cumulative problems 3, 4d, and 6.
Each problem was worth 5 points, but only the two best scores of each group were retained. The maximum number of points was therefore 20.
I was happy to see most everyone put in a lot of work into this final problem set. I'm sorry we didn't have time to grade more problems, but the grades people received did seem to reflect the overall work they put in and their understanding. I hope you learned a lot from doing these problems! Solutions to those not solved in the book are below. Have a great summer!

6.2. The primes less than 100 are
$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}$ and so $\pi(100) = 25$. The bounds of Theorem 6.1.6 say that $\frac{x}{\log x} < \pi(x) < 1.25506\frac{x}{\log x}$; plugging in $x = 100$ gives roughly $21.715 < 25 < 27.253$.

6.4. Using base 3, we calculate $3^{2^{2^5}} \equiv 3029026160 \pmod{2^{2^5}+1}$, so since this is not 1, it follows $2^{2^5}+1$ cannot be prime. This is too much work to compute by hand as far as I can tell, so you need to use a computer; I used the PowerMod function of Mathematica.

For base 2, we want to show that $2^{2^{2^n}} \equiv 1 \pmod{2^{2^n}+1}$ for all $n \geq 0$. Equivalently we need to show $2^{2^n}+1$ divides $2^{2^{2^n}} - 1$. The latter is a difference of two squares:
$2^{2^{2^n}} - 1 = (2^{2^{(2^n-1)}} + 1)(2^{2^{(2^n-1)}} - 1)$. Again the second factor here is a difference of two squares: $2^{2^{(2^n-1)}} - 1 = (2^{2^{(2^n-2)}} + 1)(2^{2^{(2^n-2)}} - 1)$. Continuing like this k times we get that $(2^{2^{(2^n-k)}} - 1)$ is a factor of $2^{2^{2^n}} - 1$. When $k = 2^n - n - 1$ we have that $2^{2^{(n+1)}} - 1 = (2^{2^n}+1)(2^{2^n}-1)$ is a factor of $2^{2^{2^n}} - 1$, and the result follows.

4.4. There are four words $\{00, 01, 10, 11\}$ in our cipher, and thus $4! = 24$ possible ciphers. We just need to count how many are affine linear and then divide to get the probability. However if you remember back to the solution to problem 3.15.12 on homework 6, I mentioned that for $n = 2$ all permutations are affine linear. It follows that the probability is 1 that a block cipher over $\{0, 1\}$ of block length 2 is affine linear. But we'd better prove this fact now that we're actually using it.

Let $f : \{0,1\}^2 \to \{0,1\}^2$ be the permutation; we want to show that we can write f as $f(\vec{v}) = A\vec{v} + \vec{b}$ where A is invertible. Pretend each word is a column vector. Let $\vec{b} = f(00)$. Let $\vec{a_1} = f(10) - \vec{b}$ and $\vec{a_2} = f(01) - \vec{b}$. Then if f is to be affine linear the columns of A must be $\vec{a_1}$ and $\vec{a_2}$. These will be distinct, since f is a permuation, so the only way A can not be invertible is if either $a_1 = \vec{0}$ or $a_2 = \vec{0}$, but these cases are also impossible since they would again imply f is not a permutation. Finally since $A\vec{v} + \vec{b}$ is injective (and thus a bijection) when A is invertible we must have $f(11) = A(11) + \vec{b}$. Therefore $f(\vec{v})$ can be written as $A\vec{v} + \vec{b}$ for an arbitrary permutation f.

Another way this could be solved is by counting the number of affine linear ciphers and showing there are also 24 distinct ones. There are 3 possible vectors that could be first column of A since the zero vector is not allowed if A is to be nonsingular. Once the first column is chosen then there are two possible vectors for the second column since we cannot choose either zero or the vector of the first column. So there are 6 choices for A. For each A we can choose 4 choices of b, making 24 possible affine linear ciphers. I'll leave it as an exercise to show that each of these 24 possibilities results in a distinct permuation.

4.6. If $p \geq 9/10$ then $q = 1 - p \leq 1/10$. From (4.2), we need to find k such that $e^{-k(k-1)/(2\cdot 365)} \leq 1/10$. Taking the logarithm of both sides gives $-k(k-1)/730 \leq -\log 10$, or $k^2 - k \geq 730 \cdot \log 10$. Solving $k^2 - k - 730 \cdot \log 10 = 0$ by the quadratic formula we get $k = (1 \pm \sqrt{1 + 2920 \log 10})/2$, so $k \geq (1 + \sqrt{1 + 2920 \log 10})/2$ suffices to give the desired probability (notice that this is the same as (4.3) with $n = 365$ except the $\log 2$ is replaced by $\log 10$ here). Approximating the value we see that $k = 42$ is sufficient for $p \geq 9/10$.

10.2. For a fixed $\pi \in S_3$ and $x \in \{0,1\}^3$, define $f_x^\pi : \{0,1\}^3 \to \{0,1\}^3$ to be $f_x^\pi(y) = h_\pi(x,y) = e_\pi(x) \oplus y$. Then f_x^π is a bijection; in fact its inverse is itself. This means that given a permutation π and a fixed x, as we vary y among all elements of $\{0,1\}^3$ we get as output all elements of $\{0,1\}^3$ exactly once. Thus for a fixed π, for each pair (x,x') where $x \neq x'$ we'll have 8 collisions as we vary the y parameter for each over all possible strings. As there are $\binom{8}{2} = 28$ such pairs (x,x') (the order doesn't matter), this gives $28 \cdot 8 = 224$ collisions per permutation π.

10.4. We have $r = 6 - 3 = 3$. The original string is 0101010101011. We first prepend two zeros to make the length divisible by 3, and then append three zeros. This results in 000 101 010 101 011 000. The length of the original string was 13, or 1101 in base 2. We split this as 11 01 and prepend a 1 to each part, giving 111 101. Our complete string is thus $x = 000\ 101\ 010\ 101\ 011\ 000\ 111\ 101$. With h_π as our compression function, we then calculate

$$\begin{aligned}
H_0 &= 000 \\
H_1 &= h_\pi(000\ 000) = 000 \oplus 000 = 000 \\
H_2 &= h_\pi(000\ 101) = 000 \oplus 101 = 101 \\
H_3 &= h_\pi(101\ 010) = 101 \oplus 010 = 111 \\
H_4 &= h_\pi(111\ 101) = 111 \oplus 101 = 010 \\
H_5 &= h_\pi(010\ 011) = 010 \oplus 011 = 001 \\
H_6 &= h_\pi(001\ 000) = 100 \oplus 000 = 100 \\
H_7 &= h_\pi(100\ 111) = 001 \oplus 111 = 110 \\
H_8 &= h_\pi(110\ 101) = 011 \oplus 101 = 110.
\end{aligned}$$

It follows $h(x) = 110$.

11.2. Neither is a problem because they are only used to determine the original text given the cipher text; they do not appear to compromise the decryption exponent d or aid forgery.

11.4. We have $n = 28829 = 127 \cdot 227$. With $p = 127$, $q = 227$, and $c = 10101$, we compute $m_p = c^{(p+1)/4} \bmod p = 103$ and $m_q = c^{(q+1)/4} \bmod p = 121$. Via the extended Euclidean algorithm we have $y_p = -84$ and $y_q = 47$. We now calculate $r = (y_p p m_q + y_q q m_p) \bmod n = 9882$ and $s = (y_p p m_q - y_q q m_p) \bmod n = 3072$. Then any of $\pm r$ or $\pm s$ can be used as the digital signature. Check that when squared each is congruent to 10101 mod n.

11.8. First calculate $h(x)^{-1} = 2095 \bmod p - 1$ using extended Euclid. Next compute $u = 99 \cdot 2095 \bmod p - 1 = 1693 \bmod p - 1$. Then $s' = su \bmod p - 1 = 1859 \bmod p - 1$. Using the CRT calculate $r' = 3052067$. So the signature is $(r', s') = (3052067, 1859)$.

1. As in the second problem of quiz 3, $\phi(\phi(n))$ represents the number of possible encryption exponents for an RSA cipher with modulus n. If $\phi(n)$ can be computed given n then RSA can be broken because $de \equiv 1 \pmod{\phi(n)}$, so given e and $\phi(n)$ we can compute the decryption exponent d using the extended Euclidian algorithm.

2. I will use the approximation $\pi(x) \sim \frac{x}{\log x}$, although other valid approximations are also fine. Then $\pi(10^5) \approx 8686$ and $\pi(10^6) \approx 72382$, and the number of primes in $[10^5, 10^6]$ is approximately $72382 - 8686 = 63696$. The probability that a randomly chosen integer in $[10^5, 10^6]$ (note that we are probably chosing 6 digit numbers here, so we wouldn't pick 10^6; of course it is not prime anyway!) is prime is then $\frac{63696}{10^6 - 10^5} \approx 0.071$. The probability that we pick n numbers at random in this interval and they are all not prime is approximately $(1 - 0.071)^n$. We calculate $(1 - 0.071)^9 \approx 0.515$ and $(1 - 0.071)^{10} \approx 0.479$, so we must pick 10 numbers to ensure the probability that at least one is prime is at least 0.5.

3. $10^6 = [F4240]_{16}$.

4. (a) Let g be a primitive root of $(\mathbb{Z}/p\mathbb{Z})^*$. Then if $x^2 \equiv 1 \pmod{p}$, it follows $g^{2k} \equiv 1 \pmod{p}$ where $g^k \equiv x \pmod{p}$. It follows the order of g, which is $p-1$, divides $2k$, and since $0 \leq k < p-1$ the only possibilities are $k = 0$ and $k = \frac{p-1}{2}$. The former results in $x = g^0 = 1 \pmod{p}$ and the latter results in $x = g^{(p-1)/2} \equiv -1 \pmod{p}$.

   (b) Note that there is only one element of $(\mathbb{Z}/2\mathbb{Z})^*$, namely 1 mod 2, and its square is 1. By the Chinese Remainder Theorem, an element x mod $2p$ satisfies $x^2 \equiv 1 \pmod{2p}$ iff $x_2^2 \equiv 1 \pmod{2}$ and $x_p^2 \equiv 1 \pmod{p}$, where (x_2, x_p) is the pair corresponding to x under the CRT bijection between $(\mathbb{Z}/2p\mathbb{Z})^*$ and $(\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*$ (concretely $x_2 = x \bmod 2$ and $x_p = x \bmod p$). Since there is only one x_2 whose square is 1 (namely 1 mod 2) and two x_p whose square is 1 (namely ± 1 mod p, we have exactly two pairs $(1,1)$ and $(1,-1)$ in $(\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*$ whose square is $(1,1)$. These correspond to ± 1 mod $2p$ in $(\mathbb{Z}/2p\mathbb{Z})^*$.

   (c) There are only two elements of $(\mathbb{Z}/4\mathbb{Z})^*$, ± 1 mod 4, and both squared give 1.

   (d) Factor square-free $n = p_1 \cdots p_r$ into a product of prime powers, where the p_i are distinct; by the CRT the number of solutions to $x^2 \equiv 1 \pmod{n}$ is the product of the number of solutions to $x^2 \equiv 1 \pmod{p_i}$ for $k = 1, \ldots, r$. Any n not of one of the forms in parts (a) to (c) must be have at least 2 odd primes dividing it. In this case by the CRT it follows the number of solutions to $x^2 \equiv 1 \pmod{n}$ is at least four.

   (e) Let $f(n)$ be the number of solutions to $x^2 \equiv 1 \pmod{n}$. If n is square-free then let $n = 2^k \cdot p_1 \cdots p_r$ where the p_i are distinct odd primes and $k \in \{0, 1\}$. Then via the CRT and the results we've established above, $f(n) = 2^r$.

   The case for more general n uses more advanced mathematics than we've covered in this course.

5. The input text is $m_1 = 101101$ and $m_2 = 110101$. The encryption key is $k = 7$.

   We have

$$\begin{aligned} c_0 &= 100111 \\ c_1 &= E_7(c_0 \oplus m_1) = 7 \cdot [001010]_2 \bmod 64 = [000110]_2 \bmod 64 \\ c_2 &= E_7(c_1 \oplus m_2) = 7 \cdot [110011]_2 \bmod 64 = [100101]_2 \bmod 64. \end{aligned}$$

   The ciphertext is then $c = 000110\ 100101$.

   For the CFB case, the ciphertext is $c_1 = 110$, $c_2 = 110$, $c_3 = 010$, and $c_4 = 011$. We have $I_1 = 100111$, $O_1 = E_7(I_1) = 7 \cdot [100111]_2 \bmod 64 = [010001]_2$, $t_1 = 010$ and $m_1 = c_1 \oplus t_1 = 100$.

   Next $I_2 = 111110$, $O_2 = 110010$, $t_2 = 110$ and $m_2 = 000$. Next $I_3 = 110110$, $O_3 = 111010$, $t_3 = 111$ and $m_3 = 101$. Finally $I_4 = 110010$, $O_4 = 011110$, $t_4 = 011$ and $m_4 = 000$. The decrypted message is then $m = 100\ 000\ 101\ 000$.

6. The order of π is the smallest $k > 0$ such that $\pi^k = I$, where I is the identity permutation. Let's write π in cycle notation so that it's easier to see what's going on: $\pi = (1234)(59867)$. If you're not familiar with cycle notation compare it to the original notation and see if you can figure it out; otherwise look in an abtract algebra text. We see here clearly that π is made up of disjoint cycles of length 4 and 5. The cycle of length 4 returns to the identity every 4th power of π, and the cycle of length 5 returns to the identity every 5th power of π. The order of π is therefore $\mathrm{lcm}(4,5) = 20$. We could use π in a Caesar cipher in which we first encode the text base 9 and then encrypt each base 9 "digit" using π.