---

[14] 1. Recall $d(n)$ is the number of divisors of n, $\sigma(n)$ is the sum of the divisors of n and $\phi(n)$ is the Euler phi function. ($169884 = 2^2 \cdot 3^3 \cdot 11^2 \cdot 13$)

(a) What is $d(169884)$? $\sigma(169884)$? $\phi(169884)$?

(b) Show that if $d(n)$ is odd then n is a square.

(c) Prove that if $c \mid ab$ and $(c, a) = d$ then $c \mid db$.

[12] 2. Find all solutions to the following Diophantine equations:

(a) $2743 \quad x + 663 \quad y \quad = \quad 42$

(b) $2166 \quad x + 678 \quad y \quad = \quad 42$

[10] 3. Prove the following is true for $n \geq 1$ using induction:

$$1 + 4 + 7 + 10 + \ldots + (6n - 2) = n(6n - 1)\,.$$

[12] 4. Write as a single congruence (if possible):

$x \equiv 3 \mod 43$
$x \equiv 5 \mod 47$
$x \equiv 27 \mod 107$

[20] 5. (a) i. State Fermat's Theorem.

ii. Find the least residue of $187^{2\,312}$ (mod) 463.

(b) i. State Eulers's Theorem.

ii. Find the least residue of $187^{2\,312}$ (mod) 468.

(c) i. State Wilson's Theorem.

ii. Find the least residue of 453! (mod) 457.

(d) i. State Gauss's Lemma.

ii. Use Gauss's Lemma to find if 7 is a quadratic residue or nonresidue modulo 19.

[18] 6. Calculate the following Legendre Symbols:

(a) $\left(\dfrac{169884}{751}\right)$ (Recall $169884 = 2^2 \cdot 3^3 \cdot 11^2 \cdot 13$)

(b) $\left(\dfrac{733}{787}\right)$

(c) $\left(\dfrac{579}{727}\right)$

[20] 7. (a) How many primitive roots does the prime 79 have?

(b) Show that 3 is a primitive root of 79.

(c) List two other primitive roots. (How do you know they are primitive roots?)

(d) Given that $3^9 = 19683 = 79(229) + 12$, what is the order of 12 mod 79? What is the order of 36 mod 79?

[14] 8. (a) Are any of the following numbers k-perfect? If so, for what value of k? (Hint: the primes in the prime power decomposition of the following are all less than 50)

i. 32760

ii. 27720

iii. 523776

(b) If n is odd and 4-perfect, is $4n$ k-perfect? If so, for what value of k? (Justify your steps carefully!)

[10] 9. (a) For an RSA encryption scheme, the publicly listed (N,e) pair is $(2257, 997)$. Find the secret decrypt key.

(b) You have intercepted the coded message 1761, decode it.

[20] 10. (a) Use Euler's Criterion to show:
If p is an odd prime, then

$$\left(\frac{-1}{p}\right) = 1 \quad \text{if} \quad p \equiv 1 \pmod{4}$$

and

$$\left(\frac{-1}{p}\right) = -1 \quad \text{if} \quad p \equiv 3 \pmod{4}$$

Question continued on next page.

(b) Find a similar formula for deciding if -2 is a quadratic residue or nonresidue modulo p where p is an odd prime.
(Hint: this should be in terms of modulo 8.)

(c) For what values of p (modulo 8) is it possible for both 2 and $p-2$ to be primitive roots of p?

The following is a list of all primes less than 1000

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	101	103	107	109	113	127	131
137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263
269	271	277	281	283	293	307	311
313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457
461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569
571	577	587	593	599	601	607	613
617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719
727	733	739	743	751	757	761	769
773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881
883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997