5.2 Fermat's Factorization Method

Note Title 4/27/2005

Problems 5-2

1. Use Fermat's method to factor each number

(a). 2229

$$47^2 < 2229 < 48^2 \qquad \frac{2229+1}{2} = 1140$$

$$\therefore 48^2 - 2229 = 25 = 5^2$$

$$\therefore 48-5 = 43, \quad 48+5 = 53$$

$$\therefore 2229 = 43 \cdot 53$$

(b) 10541 $\qquad 102^2 < 10541 < 103^2, \quad \dfrac{10541+1}{2} = 5271$

$$\therefore 103^2 - 10541 = 68$$

$$104^2 - 10541 = 275$$

$$105^2 - 10541 = 484 = 22^2$$

$$\therefore 105-22 = 83, \quad 105+22 = 127$$

$$\therefore 10541 = 83 \cdot 127$$

(c) 340663 $\qquad 583^2 < 340663 < 584^2, \quad \dfrac{340663+1}{2} = 170332$

$$584^2 - 340663 = 393$$

	A	B	C	D	E
1	k	k^2	340663	k^2 - 340663	sqrt()
2	584	341056	340663	393	19.82423
3	585	342225	340663	1562	39.52215
4	586	343396	340663	2733	52.2781
5	587	344569	340663	3906	62.498
6	588	345744	340663	5081	71.28113
7	589	346921	340663	6258	79.10752
8	590	348100	340663	7437	86.23804
9	591	349281	340663	8618	92.83318
10	592	350464	340663	9801	99

From spreadsheet,

$592^2 - 340663 = 9801$
$= 99^2$

$\therefore 592 - 99 = 493, \; 592 + 99 = 691$

691 is prime (from table of primes), 493 not

$\therefore 22^2 < 493 < 23^2, \; \frac{493+1}{2} = 247$

$23^2 - 493 = 36 = 6^2$

$\therefore 23 + 6 = 29, \; 23 - 6 = 17$

$\therefore 493 = 17 \cdot 29$

$\therefore 340663 = 17 \cdot 29 \cdot 691$

2. Prove a perfect square must end in one of the following digits:

00	16	29	49	69	89
01	21	36	56	76	96
04	24	41	61	81	
09	25	44	64	84	

Pf: First note $(x+50)^2 = x^2 + 100x + 2500$, so $x^2 \equiv (x+50)^2 \pmod{100}$. This means you only need to examine last two digits of $x = 0, 1, 2, \ldots, 49$ since $0^2 \equiv 50^2$, $1^2 \equiv 51^2$, ...

But $(x-50)^2 = x^2 - 100x + 2500$, so $x^2 \equiv (x-50)^2 \pmod{100}$

$\therefore x^2 \equiv (50-x)^2 \pmod{100}$, so for $x = 26, 27, \ldots, 49$

$26^2 \equiv 24^2$, $27^2 \equiv 23^2$, $\ldots$ $49^2 \equiv 1^2$.

$\therefore$ Only need to look at digits $x = 0, 1, 2, \ldots, 25$

x	$x^2 \pmod{100}$	x	$x^2 \pmod{100}$	x	$x^2 \pmod{100}$
0	00	10	00 *	20	00 *
1	01	11	21	21	41
2	04	12	44	22	84
3	09	13	69	23	29
4	16	14	96	24	76
5	25	15	25 *	25	25 *
6	36	16	56		
7	49	17	89		
8	64	18	24		
9	81	19	61		

* = duplicated ending

$\therefore$ The above endings are the ones that were to be proved.

3. Factor the number $2^{11}-1$ using Fermat's method.

$2^{11}-1 = 2047$, $45^2 < 2047 < 46^2$

From spreadsheet, $56^2 - 2047 = 1089 = 33^2$

	A	B	C
1	x	x^2 -2047	sqrt()
2	46	69	8.306624
3	47	162	12.72792
4	48	257	16.03122
5	49	354	18.81489
6	50	453	21.2838
7	51	554	23.5372
8	52	657	25.63201
9	53	762	27.60435
10	54	869	29.47881
11	55	978	31.27299
12	56	1089	33
13	57	1202	34.66987

$\therefore\ 56^2 - N^2 = 33^2, \quad N = (56+33)(56-33),$

or $N = 89 \cdot 23$

$\therefore\ 2^{11} - 1 = 89 \cdot 23$

4. If $n^2 = a^2 + b^2 = c^2 + d^2$, $\gcd(a,b) = \gcd(c,d) = 1$,

Then
$$n = \frac{(ac+bd)(ac-bd)}{(a+d)(a-d)}$$

(a). Factor $493 = 18^2 + 13^2 = 22^2 + 3^2$

$$493 = \frac{(18 \cdot 22 + 13 \cdot 3)(18 \cdot 22 - 13 \cdot 3)}{(18+3)(18-3)} = \frac{(435)(357)}{(21)(15)}$$

$$= \frac{435}{15} \cdot \frac{357}{21} = 29 \cdot 17$$

(b) $38025 = 168^2 + 99^2 = 156^2 + 117^2$

$$= \frac{(168 \cdot 156 + 99 \cdot 117)(168 \cdot 156 - 99 \cdot 117)}{(168+117)(168-117)}$$

$$= \frac{(37791)(14625)}{(285)(51)} = \frac{14625}{285} \cdot \frac{37791}{51}$$

$$= \frac{14625}{285} \cdot 741$$

But 741 is not prime: $741 = 3 \cdot 247 = 3 \cdot 13 \cdot 19$

$$\therefore 38025 = \frac{14625}{285} \cdot (3 \cdot 13 \cdot 19)$$

$\frac{14625}{285}$ is not an integer

$$\frac{14625}{285} = \frac{5 \cdot 2925}{5 \cdot 57} = \frac{25 \cdot 117}{3 \cdot 19} = \frac{5^2 \cdot 9 \cdot 13}{3 \cdot 19}$$

$$\therefore 38025 = \frac{5^2 \cdot 9 \cdot 13}{3 \cdot 19} \cdot 3 \cdot 13 \cdot 19$$

$$= \frac{5^2 \cdot 3^2 \cdot 13}{19} \cdot 13 \cdot 19$$

$$= 3^2 \cdot 5^2 \cdot 13^2$$

5. Use generalized Fermat method to factor.

(a). 2911 Use hint: $138^2 \equiv 67 \pmod{2911}$

$$\therefore \gcd(138-67, 2911) = \gcd(71, 2911)$$

Using Euclidean Algorithm,

$\underline{2911 = 41 \cdot 71}$, and 71 & 41 both prime.

(b) 4573 Use hint: $177^2 \equiv 92^2 \pmod{4573}$

$\therefore \gcd(177-92, 4573) = \gcd(85, 4573)$

$\therefore 4573 = 53 \cdot 85 + 68$

$85 = 1 \cdot 68 + 17$

$68 = 4 \cdot 17 \qquad \therefore \gcd = 17$

$\gcd(177+92, 4573) = \gcd(269, 4573)$

$\therefore 4573 = 17 \cdot 269, \quad \therefore \gcd = 17$

Also, 269 is prime, $\therefore \underline{4573 = 17 \cdot 269}$

(c) 6923 From hint: $208^2 \equiv 93^2 \pmod{6923}$

$\therefore \gcd(208-93, 6923) = \gcd(115, 6923)$

$\therefore 6923 = 60 \cdot 115 + 23$

$115 = 5 \cdot 23 \qquad \therefore \gcd = 23$

$\gcd(208+93, 6923) = \gcd(301, 6923)$

$\therefore 6923 = 23 \cdot 301, \therefore \gcd = 301$

and $301 = 7 \cdot 43$

$\therefore \underline{\underline{6923 = 7 \cdot 23 \cdot 43}}$

6. Factor 13561

From $233^2 \equiv 8^2 \cdot 5 \pmod{13561}$,
$1281^2 \equiv 2^4 \cdot 5 \pmod{13561}$

$(233 \cdot 1281)^2 \equiv 2^4 \cdot 3^2 \cdot 5^2 = (2^2 \cdot 3 \cdot 5)^2 \pmod{13561}$

$\therefore 298473^2 \equiv 60^2 \pmod{13561}$

and $298473 - 22 \cdot 13561 = 131 \not\equiv \pm 60 \pmod{13561}$

$\therefore \gcd(298473 - 60, 13561) = \gcd(298413, 13561)$

$298413 = 22 \cdot 13561 + 71$

$13561 = 191 \cdot 71$, $\therefore \gcd = 71$ (a prime)

and 191 is prime.

$\therefore \underline{\underline{13561 = 71 \cdot 191}}$

7. (a). Factor 4537 by searching for x s.t. $x^2 - k \cdot 4537$ is the product of small primes.

$\sqrt{4537} = 67.4$

$\therefore\ 67^2 - 4537 = -48 = -2^4 \cdot 3$ [1]

$68^2 - 4537 = 87 = 3 \cdot 29$ [1']

$\sqrt{2 \cdot 4537} = 95.3$

$95^2 - 2 \cdot 4537 = -49 = -7^2$ [2]

$96^2 - 2 \cdot 4537 = 142 = 2 \cdot 71$ [2']

$\sqrt{3 \cdot 4537} = 116.7$

$116^2 - 3 \cdot 4537 = -155 = -5 \cdot 31$ [3]

$117^2 - 3 \cdot 4537 = 78 = 2 \cdot 3 \cdot 13$ [3']

$\sqrt{4 \cdot 4537} = 134.7$

$134^2 - 4 \cdot 4537 = -192 = -2 \cdot 2 \cdot 48 = -2^6 \cdot 3$ [4]

$135^2 - 4 \cdot 4537 = 77 = 7 \cdot 11$ [4']

Note: gcd = 1 from [1], [4]

$\sqrt{5 \cdot 4537} = 150.6$

$150^2 - 5 \cdot 4537 = -185 = -5 \cdot 37$ [5]

$151^2 - 5 \cdot 4537 = 116 = 4 \cdot 29$ [5']

$\sqrt{6 \cdot 4537} = 164.99$ [6]

$165^2 - 6 \cdot 4537 = 3$ [6']

$\sqrt{7\cdot 4537} = 178.2$

$178^2 - 7\cdot 4537 = -75 = -3\cdot 5^2$ [7]

$179^2 - 7\cdot 4537 = 282 = 2\cdot 141 = 2\cdot 3\cdot 47$ [7']

$\sqrt{8\cdot 4537} = 190.5$

$190^2 - 8\cdot 4537 = -196 = -2\cdot 98 = -2^2\cdot 7^2$ [8]

$191^2 - 8\cdot 4537 = 185 = 5\cdot 37$ [8']

Note: gcd = 1 from [2], [8]

gcd = 1 from [5], [8']

$\sqrt{9\cdot 4537} = 202.1$

$202^2 - 9\cdot 4537 = -29$ [9]

$\therefore$ look at [9], [5']

$\therefore (202\cdot 151)^2 \equiv (2\cdot 29)^2 \pmod{4537}$

$(30502)^2 \equiv (58)^2 \pmod{4537}$

$\gcd(30502-58, 4537) = \gcd(30444, 4537) = 1$

$\gcd(30502+58, 4537) = \gcd(30560, 4537) = 1$

$203^2 - 9\cdot 4537 = 376 = 2^3\cdot 47$ [9']

$\therefore$ look at [6'], [7'], [9']

$(165\cdot 179\cdot 203)^2 \equiv (2^2\cdot 3\cdot 47)^2 \pmod{4537}$

$(5995605)^2 \equiv (564)^2 \pmod{4537}$

$\gcd(5995605-564, 4537) = \gcd(5995041, 4537)$

$5995041 = 1321\cdot 4537 + 1664$

$4537 = 2\cdot 1664 + 1209$

$1664 = 1 \cdot 1209 + 455$
$1209 = 3 \cdot 455 - 156$
$455 = 3 \cdot 156 - 13$
$156 = 12 \cdot 13$
$\gcd = 13$

$\therefore$ $\underline{4537 = 13 \cdot 349}$, and 349 is prime

(b). Factor 14429 using method in (a).

Use hint

$120^2 - 14429 = -29$
$3003^2 - 625 \cdot 14429 = -116 = -2^2 \cdot 29$

$\therefore (120 \cdot 3003)^2 \equiv (2 \cdot 29)^2 \pmod{14429}$
$(360360)^2 \equiv (58)^2 \pmod{14429}$

$\gcd(360360 - 58, 14429) = \gcd(360302, 14429)$

$360302 = 25 \cdot 14429 - 423$
$14429 = 34 \cdot 423 + 47$
$423 = 9 \cdot 47$
$\therefore \gcd = 47$ (a prime)

$\gcd(360360+58, 14429) = \gcd(360418, 14429)$

$360418 = 25 \cdot 14429 - 307$

$14429 = 47 \cdot 307$

$\therefore \gcd = 307$

$\therefore 14429 = 47 \cdot 307$

8. Use Kraitchik's method to factor 20437

$\sqrt{20437} = 142.9$

$143^2 - 20437 = 12 \quad = 2^2 \cdot 3 \qquad [1]$

$144^2 - 20437 = 299 \quad = 13 \cdot 23$

$145^2 - \text{''} \quad = 588 \quad = 2^2 \cdot 3 \cdot 7^2 \qquad [3]$

$146^2 - \text{''} \quad = 879 \quad = 3 \cdot 293$

$147^2 - \text{''} \quad = 1172 \quad = 2^2 \cdot 293$

$148^2 - \text{''} \quad = 1467 \quad = 3^2 \cdot 163$

From [1], [3], $(143 \cdot 145)^2 = (2^2 \cdot 3 \cdot 7)^2 \pmod{20437}$

$(20735)^2 \equiv (84)^2 \pmod{20437}$

$\gcd(20735-84, 20437) = \gcd(20651, 20437)$

$20651 = 1 \cdot 20437 + 214$

$20437 = 95 \cdot 214 + 107$

$214 = 2 \cdot 107$

$\therefore \gcd = 107$ (a prime)

$\gcd(20735 + 84, 20437) = \gcd(20819, 20437)$

$\therefore 20819 = 1 \cdot 20437 + 382$

$20437 = 53 \cdot 382 + 191$

$382 = 2 \cdot 191$

$\therefore \gcd = 191$ (a prime)

$\therefore \underline{20437 = 107 \cdot 191}$