1.) 3.22

(a) $n = 1739$ $a = 2$

$\underline{n=2}$ $2^{2!} = 2^2 \equiv 4 \pmod{1739} \rightarrow \gcd(3, 1739) = 1$

$1739 = 3(579) + 2$

$3 = 2(1) + \underline{1} \leftarrow$ GCD

$2 = 1(2) + 0$

$\underline{n=3}$ $2^{3!} \equiv (2^{2!})^3 \equiv 4^3 \equiv 64 \pmod{1739} \rightarrow \gcd(63, 1739) = 1$

$1739 = 63(27) + 38$

$63 = 38(1) + 25$

$38 = 25(1) + 13$

$25 = 13(1) + 12$

$13 = 12(1) + 1 \leftarrow$ GCD

$12 = 1(12) + 0$

$\underline{n=4}$ $2^{4!} \equiv (2^{3!})^4 \equiv 64^4 \equiv 1083 \pmod{1739} \rightarrow \gcd(1082, 1739) = 1$

$1739 = 1082(1) + 657$

$1082 = 657(1) + 425$

$657 = 425(1) + 232$

$425 = 232(1) + 193$

$232 = 193(1) + 39$

$193 = 39(4) + 37$

$39 = 37(1) + 2$

$37 = 2(18) + \underline{1} \leftarrow$ GCD

$2 = 1(2) + 0$

$\underline{n=5}$ $2^{5!} \equiv 1083^5 \equiv 1395 \bmod (1739) \rightarrow \gcd(1394, 1739) = 1$

$1739 = 1395(1) + 344$

$1395 = 344(4) + 19$

$344 = 19(18) + 2$

$19 = 2(9) + \underline{1}$

$2 = 1(2) + 0$

$\underline{n=6}$ $2^{6!} \equiv 1395^6 \equiv 1444 \rightarrow \gcd(1443, 1739) = \boxed{37}$ stop!

$1739 = 1443(1) + 296$

$1443 = 296(4) + 259$

$296 = 259(1) + \underline{37} \leftarrow$ gcd

$259 = 37(7) + 0$

$\rightarrow p = 37$

$q = \frac{N}{p} = \frac{1739}{37} = 47$

$1739 = 37 \cdot 47$

2) 3.22

(b) $n = 220459$

$n=2$ | $2^{2!} \equiv 4 \bmod 220459 \to \gcd(3, 220459) = \underline{1}$

$n=3$ | $2^{3!} \equiv 4^3 \equiv 64 \bmod 220459 \to \gcd(63, 220459) = \underline{1}$

$n=4$ | $2^{4!} \equiv 64^4 \equiv 22332 \to \gcd(22331, 220459) = \underline{1}$

$n=5$ | $2^{5!} \equiv 22332^5 = 85054 \pmod{220459} \to \gcd(85053, 220459) = \underline{1}$

$n=6$ | $2^{6!} \equiv 85054^6 \equiv 4046 \pmod{220459} \to \gcd(4045, 220459) = \underline{1}$

$n=7$ | $2^{7!} \equiv 4046^7 \equiv 43103 \pmod{220459} \to \gcd(43102, 220459) = \underline{1}$ ✓

$n=8$ | $2^{8!} \equiv 179601 \bmod 220459 \to \gcd(179600, 220459) = \underline{449}$

Stop!

$\to p = 449$

$$q = \frac{N}{p} = \frac{220459}{449} = 491$$

$220459 = 449 \cdot 491$

3. 3.24

(a) $N = 53357$

Perfect Square?

$53357 + 1^2 = 53358$ ✗

$53357 + 2^2 = 53361$ ✓

$53361 = 231^2$

$N = 231^2 - 2^2 = (231+2)(231-2)$

$= 233 \cdot 229$

(b) $N = 34571$

$34571 + 1^2 = 34572$ ✗

$34571 + 2^2 = 34575$ ✗

$34571 + 3^2 = 34580$ ✗

$34571 + 4^2 = 34587$ ✗

$34571 + 5^2 = 34596 = 186^2$ ✓

$\rightarrow N = 186^2 - 5^2 = (186+5)(186-5)$

$N = 191 \cdot 181$

(c) $N = 25777$

$25777 + 1^2 = 25778$ ✗

$25777 + 2^2 = 25781$ ✗

$+3^2 = 25786$ ✗

$+4^2 = 25793$ ✗

$+5^2 = 25802$ ✗

$+6^2 = 25813$ ✗

$+7^2 = 25826$ ✗

$+8^2 = 25841$ ✗

$+9^2 = 25858$ ✗

$+10^2 = 25877$ ✗

$+11^2 = 25898$

$+12^2 = 25921 = 161^2$ ✓

$\rightarrow N = 161^2 - 12^2$

$= (161-12)(161+12)$

$N = 149 \cdot 173$

4. 3.26

(a) $N = 61063$

$$1882^2 \equiv 270 \equiv 2 \cdot 3^3 \cdot 5 \pmod{61063}$$
$$1898^2 \equiv 60750 \equiv 2 \cdot 3^5 \cdot 5^3$$

$$1882^2 \cdot 1898^2 \equiv 2^2 \cdot 3^8 \cdot 5^4 \pmod{61063}$$
$$(1882 \cdot 1898)^2 \equiv (2 \cdot 3^4 \cdot 5^2)^2$$
$$(\underbrace{3572036}_{a})^2 \equiv (\underbrace{4050}_{b})^2$$

$$a-b = 3572036 - 4050 = 3567986$$

$$\gcd(N, a-b) = \gcd(61063, 3567986) = 227$$

$$q = \frac{N}{p} = \frac{61063}{227} = 269 \qquad N = 227 \cdot 269$$

(b) $N = 52907$

$$763^2 \equiv 192 \equiv 2^6 \cdot 3$$
$$773^2 \equiv 15552 \equiv 2^6 \cdot 3^5$$
$$763^2 \cdot 773^2 \equiv 2^{12} \cdot 3^6 \pmod{52907}$$
$$(763 \cdot 773)^2 \equiv (2^6 \cdot 3^3)^2$$
$$(\underbrace{589799}_{a})^2 \equiv (\underbrace{1728}_{b})^2$$

$$a-b = 589799 - 1728 = 588071$$

$$\gcd(N, a-b) = \gcd(52907, 588071) = 277$$

$$52907 = 191 \cdot 277$$

4.

$$1189^2 \equiv 27000 \equiv 2^3 \cdot 3^3 \cdot 5^3$$
$$1605^2 \equiv 686 \equiv 2 \cdot 7^3$$
$$2815^2 \equiv 105 \equiv 3 \cdot 5 \cdot 7$$

$$1189^2 \cdot 1605^2 \cdot 2815^2 \equiv 2^4 \cdot 3^4 \cdot 5^4 \cdot 7^4$$
$$\equiv (2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2)^2$$

$$5371991175 \equiv 44100$$

$$a - b = 5371947075$$

$$\gcd(198103, 5371947075) = 499$$

$$198103 = 397 \cdot 499$$

5. $p^e \leq 10$

- $2^1 = 2$
- $2^2 = 4$
- $2^3 = 8$
- $3^1 = 3$
- $3^2 = 6$
- $5^1 = 5$
- $7^1 = 7$

$$n = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 8 \cdot 9 \cdot 5 \cdot 7$$

LARGEST 10-powersmooth #: 2520

6.

	24	35	51	52	76	210
	$\downarrow 2$			$\downarrow 2$	$\downarrow 2$	$\downarrow 2$
	12	35	51	26	38	105
	$\downarrow 3$		$\downarrow$			$\downarrow$
	4	35	17	26	38	35
	$\downarrow 4$					
	1	35	17	26	38	35
		$5\downarrow$				$\downarrow$
		7	17	26	38	7
$6\downarrow$						
		7	17	26	38	7
$7\downarrow$						
		1	17	26	38	1
$8\downarrow$						
			17	26	38	

$$24 = 2^3 \cdot 3$$
$$35 = 5 \cdot 7$$
$$210 = 2 \cdot 3 \cdot 5 \cdot 7$$